TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JOUNI VEIMA

MOBIILISOVELLUSTEN KEHITYS TERVEYDENHUOLLON TARPEISIIN

Diplomityö

Tarkastaja: professori Kari Systä
Tarkastaja ja aihe hyväksytty
30. marraskuuta 2017

TIIVISTELMÄ

JOUNI VEIMA: Mobiilisovellusten kehitys terveydenhuollon tarpeisiin
Tampereen teknillinen yliopisto
Diplomityö, 59 sivua, 0 liitesivua
Lokakuu 2018
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Ohjelmistotuotanto
Tarkastaja: Professori Kari Systä

Avainsanat: mobiili, sovellus, terveydenhuolto, CE-merkintä, android, iOS, mobiilikäyttöjärjestelmä, mobiiliteknologia, tietoturva.

Työn tarkoituksena on selvittää mitä tulee ottaa huomioon, kun suunnitellaan ja toteutetaan mobiilisovelluksia terveydenhuollon tarpeisiin. Työ jakautuu kahteen osaan. Ensimmäisessä osassa käydään läpi mobiilin terveydenhuollon ominaisuudet. Työssä selvitetään mitä on mobiili terveydenhuolto, miten mobiililaitteet toimivat terveydenhuollon sovellusten alustana ja miten terveydenhuollon lait ja säädökset vaikuttavat kehitykseen. Lakien soveltamisen näkökulmasta käsitellään lääkinnällisten laitteiden määritelmät, luokat, luokittelu perusteet, miten eri luokitukset vaikuttavat, sekä mitä vaaditaan, että laite voidaan asettaa markkinoille Euroopan Unionin alueella. Erityisesti mikä on CE-merkintä ja mitä tulee tehdä, että se voidaan laillisesti kiinnittää laitteeseen. Terveydenhuoltoon liittyvän osuuden lopussa käsitellään vielä, miksi hyvä tietoturva on erityisen tärkeä vaatimus terveydenhuollon sovelluksissa.

Työn toinen osa käsittelee mobiilisovellusten kehittämistä yleisesti. Työssä käydään läpi kaksi suurinta mobiilikäyttöjärjestelmää ja niiden ominaisuudet sovellusten kehitykseen liittyen, kolme eri mobiiliteknologiaa ja sovellusten jakaminen ja julkaisu sovelluskaupoissa ja itsenäisesti. Näiden lisäksi tutkitaan mobiilikehityksen yleisiä haasteita, kuten laitteiden pientä kokoa, mobiilisovellusten suuria laatuvaatimuksia, useiden erilaisten alustojen tukemista ja huonoja tietoliikenneyhteyksiä, sekä erilaisia ratkaisuja näiden haasteiden ratkaisemiseksi. Lopuksi käydään läpi mobiiliuhkia, niiltä suojautumista ja muita mobiilisovellusten tietoturvaan liittyviä piirteitä.

ABSTRACT

JOUNI VEIMA: Development of mobile applications for health care
Tampere University of Technology
Master of Science Thesis, 59 pages, 0 Appendix pages
October 2018
Master's Degree Programme in Information Technology
Major: Software Engineering
Examiner: Professor Kari Systä

Keywords: mobile, application, health care, CE marking, android, iOS, mobile operating system, mobile technology, information security.

The purpose of this thesis is to examine what needs to be taken into account when a company starts to develop mobile applications for healthcare. The thesis is divided into two parts. The first part focuses on the properties of mobile healthcare. The thesis will provide answers to what mobile healthcare is, how mobile devices work as a platform for healthcare applications and how the laws and requirements of healthcare affect on development. In the thesis the following are explained definitions of healthcare devices, different categories of healthcare devices, category definitions, how the categories affect and what is required before the device can be sold at the European Union region. Especially what is CE marking and the requirements to attach it to the product. In the end of the first section of the thesis is explained why information security is very important in healthcare applications.

The second part of the thesis is about mobile development in general. The two biggest mobile operating systems and their application programming properties, three mobile technologies and publishing and sharing in application stores or independently are examined. Additionally, common challenges in mobile application development such as the small size of devices, big quality requirements, supporting many different platforms and bad connections and how to solve them are examined. Finally, mobile threats, how to protect against them and other mobile information security features are considered.

ALKUSANAT

Pitkä taival on viimein ohi. Vaikka elämä onkin ainaista oppimista, niin tähän päättyy ainakin toistaiseksi koulun penkillä istuminen ja siirryn innokkaasti kohti työelämän haasteita. Opiskeluaikani Tampereen teknillisessä yliopistossa oli todella tapahtumarikas ja opittujen asioiden lisäksi mieleen painuu roppakaupalla kultaisia muistoja. Tahdon kiittää koko sydämestäni perhettäni ja ystäviäni, jotka auttoivat ja tukivat pitkän taipaleen aikana ja tämänkin diplomityön tekemisessä. Kiitos suuresti työn tarkastajalle kaikesta avusta ja huolenpidosta. Haluan kiittää myös työnantajaani, jonka kautta sain aiheen työlle ja tukea sen tekemiseen.

Tampereella, 31.7.2018

Jouni Veima

SISÄLLYSLUETTELO

KUVALUETTELO

LYHENTEET JA MERKINNÄT

AMD	Active medical device. Aktiivinen lääkinnällinen laite.
API	Application programming interface. Rajapinta.
APK	Android application package. Android sovellusten asennuspaketti.
APP	Application. Sovellus.
App Store	iOS käyttöjärjestelmän sovelluskauppa.
BSN	Body sensor network. Usean laitteen luoma verkko kehon tarkkailuun.
Google Play	Android käyttöjärjestelmän sovelluskauppa.
IDE	Integrated development environment. Kehitysympäristö.
IVD	In vitro device. Laite, joka testaa ihmisestä peräisin olevaa näytettä. Esimerkiksi verinäytteitä testaavat laitteet.
Jailbreak	iOS käyttöjärjestelmän mobiililaitteelle suoritettava operaatio, jolla voidaan muokata käyttöjärjestelmää esimerkiksi rajoitusten kiertämiseksi. (1)
macOS	Applen luoma ja markkinoima käyttöjärjestelmä.
MAM	Mobile application management. Mobiilisovellusten hallinnointiohjelma.
MBaaS	Mobile back-end as a service. Palvelu, joka tarjoaa mobiilisovelluksille suunnattuja Back-End järjestelmiä asiakkaille.
MD	Medical device. Lääkinnällinen laite.
MDM	Mobile device management. Mobiililaitteiden hallintaohjelma.
MitM	Man in the middle attack. Väliintulohyökkäys, jossa hyökkääjä on käyttäjän ja palvelun välissä.
NANDO	New approach notified and designated organisations. Euroopan Unionin rekisteri, jossa listataan viralliset kliinistä arviointia tekevät laitokset.
NFC	Near field communication. Protokolla lähietäisyydeltä tapahtuvaan laitteiden väliseen tiedonsiirtoon.
Play Console	Sivusto, jonka kautta voidaan hallinnoida ja päivittää Android sovelluksia.
Root	Android laitteille suoritettava operaatio, jolla voidaan muokata käyttöjärjestelmää esimerkiksi rajoitusten kiertämiseksi. (1)
Vendor lock	Tilanne, jossa organisaatio on riippuvainen yhdestä toimittajasta tai teknologiasta ja toiseen vastaavaan vaihtaminen ei ole mahdollista käytettävissä olevilla resursseilla.

1. JOHDANTO

Mobiililaitteet ovat tulleet osaksi elämäämme. Meillä on aina mukana mobiililaite, joka auttaa meitä päivittäisissä tehtävissä. Mobiililaitteet avaavat täten yrityksille mahdollisuuden olla vuorovaikutuksessa, pitää yllä mielenkiintoa ja luoda uutta arvoa yrityksen asiakkaille ja työntekijöille. Mobiililaitteet eivät vaikuta vain henkilökohtaiseen osaan elämäämme. Ne ajavat myös yhteiskunnallisia muutoksia monilla toimialoilla. Yksi näistä toimialoista on terveydenhuolto. (1; 2)

Mobiiliteknologiassa on koko ajan käynnissä oleva muutostila. Uusia teknologioita ja alustoja tulee alituiseen lisää. Mobiilisovellusmarkkinoilla liikkuu huomattava määrä rahaa. App Annie sivuston tekemän analyysin mukaan 2017 vuoden viimeisen vuosineljänneksen aikana kuluttajat käyttivät yhteensä melkein 27 miljardia Yhdysvaltojen dollaria sovelluskaupoissa (3). Mobiiliteknologia ylettyy melkein jokaiseen liiketoiminnan näkökulmaan. Odotukset laadukkaille, nopeasti toimitetuille mobiilisovelluksille ovat ennennäkemättömät. Tietoturva ja yksityisyyden suojaaminen ovat keskeisessä asemassa. (1)

Terveydenhuollon sovelluksille on erityisvaatimuksia, jotka tulee ottaa huomioon kehityksessä. Potilaan tai laitteen käyttäjän terveys ei saa vaarantua. Laitteiden valmistajan tulee olla tietoinen oikeanlaisesta menettelystä laitteiden saattamiseksi markkoinoille Suomen ja Euroopan Unionin alueella ja laitteen tulee olla direktiiveissä ja laeissa olevien vaatimusten mukaisia. Lakisääteisten menettelyiden ja vaatimusten hallinta voi olla yritykselle joko kilpailuetu tai kaupaneste riippuen siitä, onko yritys itse ottanut riittävästi selvää niistä ja omaksunut ne omaan toimintaansa. (4; 5)

Mitä tulee huomioida, kun lähdetään tuottamaan sovelluksia mobiileille alustoille? Mitä haasteita mobiiliteknologioilla kehitykseen liittyy yleisesti, datan säilyttämiseen, sovellusten julkaisuun ja tietoturvaan? Mitä ovat erityisvaatimukset, joita terveydenhuoltoon keskittyminen luo? Tässä työssä etsitään vastauksia muun muassa näihin kysymyksiin ja esitellään tärkeimmät asiat, jotka kehittäjän on hyvä tietää mobiilisovellusten kehitysprosessista ja vaihtoehdoista terveydenhollon alalla ja yleisesti.

2. TUTKIMUS

2.1 Toimeksiantaja

Toimeksiantaja on suomalainen vuodesta 1995 alkaen toiminut yritys nimeltä Enersoft Oy. Enersoft Oy pääasiallisesti määrittää ja toteuttaa terveydenhuoltoon ja sairaalatekniikkaan liittyviä ohjelmistokokonaisuuksia. Kokonaisvaltainen palvelu sisältää ohjelmistojen suunnittelun, toteutuksen, ylläpidon ja jatkokehittämisen. Asiakkaita ovat sairaalat, yksityiset laboratoriot sekä energialaitokset. Yrityksen toimipiste sijaitsee Tampereella ja yrityksessä työskentelee noin 20 henkilöä. (6)

2.2 Tutkimuksen tavoitteet

Terveydenhuolto on tulevan vuosikymmenen tärkeimpiä tietotekniikan alan alueita. Monet suuret yritykset valmistautuvat tuottamaan terveydenhuoltoon liittyviä ohjelmia. Google, Apple ja Samsung ovat jo lanseeranneet omat lääketieteeseen liittyvät sovellukset: Google Fit, Heath app ja Samsung Health. (7; 8; 9; 10) Yksi terveydenhuoltoon kuin moneen muuhunkin alaan vaikuttava tekijä on ohjelmoitavat ja interaktiiviset mobiililaitteet. Mobiilista on tullut tärkeä liiketoiminta-alue monelle yritykselle. (1)

Toimeksiantaja haluaa kartoittaa mitä haasteita, mahdollisuuksia ja piirteitä mobiilille alustalle siirtymiseen liittyy. Tutkimuksen tavoitteena on selvittää ja esittää mobiilialustoille kehittämisen ominaisuudet ja haasteet. Tutkimus vastaa kysymykseen mitä tulee ottaa huomioon, kun lähdetään kehittämään terveydenhuoltoon liittyviä sovelluksia mobiilialustoille. Tutkimus on jaettu seuraaviin osiin: Sovelluksen kehitys itsessään, kehityksen haasteet, jakelu ja tietoturva. Tutkimus keskittyy terveydenhuoltoon liittyviin sovelluksiin, joten edellä mainittujen lisäksi käydään läpi terveydenhuoltoon liittyvät vaikutukset mobiilialustoilla. Tavoitteena ei ole luoda yksityiskohtaista, kaiken määrittävää selontekoa, vaan ohjaava yleiskuva.

3. MOBIILI TERVEYDENHUOLTO

Mobiilin terveydenhuollon mahdollistaa pienet ja kevyet, mutta silti tehokkaat mobiililaitteet. Mobiililaitteiden ansioista terveydenhuolto ei rajoitu terveydenhuollon toimipisteisiin vaan liikkuu käyttäjän mukana. Ilman mobiililaitteiden apua niin potilaat kuin terveydenhuollon ammattilaiset olisivat sidottuna tiettyyn paikkaan ja tiettyyn aikaan terveydenhuollon toimia varten. Esimerkiksi potilastietojen keräys tai käsittely tehtäisiin sairaalassa terveydenhuollon laitteen ja pöytätietokoneen ääressä. (11; 12; 13; 14). Mobiililaitteiden käyttö terveydenhuoltoon liittyvien sovellusten alustana on lisääntynyt (15; 16) ja jatkaa kehittymistään (11; 17). Mobiileilla terveydenhuollon järjestelmillä on potentiaalia tulla kiinteäksi osaksi modernia terveydenhuollon järjestelmää ja ne voivat tarjota vaihtoehtoisia ratkaisuja useisiin lääketieteellisiin ja sosiaalisiin ongelmiin. Mobiilissa terveydenhuollossa on monta selvästi perinteisestä terveydenhuollosta erotettavissa olevaa osaa. Näitä ovat puettavat laitteet, käyttäjän mahdollisuus käyttää laitetetta ollessaan liikkeellä ja ennalta määrittämättömissä paikoissa, tiedon lähetys langattomasti, etänä tehtävä terveydenhuolto ja näistä seuraava terveydenhuollon joustavuus. (18)

Terveydenhuolto alustana tuo myös lisävaatimuksia mobiilisovelluksille. Terveysteknologia-alan peruslähtökohta on, että laitteen turvallisuudessa, suorituskyvyssä ja vaikuttavuudessa ei saa tehdä kompromisseja. Potilaan etu on ehdoton ja laitteen on sovelluttava käyttötarkoitukseensa. (4) Tuotteen markkinoille saattaminen Euroopan Unionin alueella sisältää monta eri vaihetta. Valmistajan on tunnettava nämä menettelyt, sekä Suomen lakien ja Euroopan Unionin direktiivien vaatimukset terveydenhuollon laitteille ja varmistaa, että tuote täyttää nämä vaatimukset.

Tässä luvussa käymme läpi, kuinka mobiililaitteet toimivat alustana terveydenhuollon sovelluksille, puettavien laitteiden ominaisuudet, mitä tulee ottaa erityisesti huomioon tietoturvan kannalta terveydenhuollon sovelluksia kehitettäessä, kuinka terveydenhuollon tuote saatetaan markkinoille Suomen tai Euroopan Unionin alueella, sekä mitkä lait ja vaatimukset koskevat terveydenhuollon sovelluksia.

3.1 Mobiili terveydenhuollon alustana

Mobiililaitteet ovat hyvä alusta terveydenhuoltoon liittyville sovelluksille useasta eri syystä. Monet mobiililaitteet kuten älypuhelimet ovat käytännössä taskukokoisia tietokoneita. Laitteiden tehokkuus ja tekninen kyvykkyys on kasvanut, mutta samalla niiden hinta on alentunut. Tämä on johtanut mobiililaitteiden laajaan käyttöönottoon ja kaikkialla läsnäolevaan käyttöön. (11; 12; 13; 15; 19). Mobiililaitteiden aktiivinen käyttö, käyttäjän mukana kulku ja ihmisten kiintyminen niihin helpottavat terveydenhuollon sovellusten sisällyttämistä kohteen päivittäisiin rutiineihin ja lisäämään positiivista tunnetta

sovellusten käyttöä kohtaan (13; 20). Laitteet ovat tietoisia niiden ympäristöstä sensorien ja henkilökohtaisen informaation kautta. Kontekstitietoisuutta voidaan käyttää hyväksi usealla eri tavalla. Laitteiden sensorien keräämää tietoa käyttäjän toimista ja tilasta voidaan esimerkiksi prosessoida laitteessa ja esittää käyttäjälle kosketusnäytöllä. (11; 12; 13; 18).

Mobiililaitteiden avulla voidaan tehdä terveydenhuollosta joustavampaa. Ennen mobiililaitteiden tuloa terveydenhuollon toimipisteinä toimivat usein vain sairaalat ja klinikat. Joihinkin operaatioihin pystyttiin käyttämään potilaan kotia toimipisteenä. Mobiililaitteiden ja langattoman yhteyden ansiosta potilaat ja terveydenhuollon ammattilaiset eivät ole enää sidottu paikkaan ja toiminta on mahdollista melkein missä ja milloin vain. (11; 12; 13; 21). Potilaan ei tarvitse pysyä sairaalassa tai terveydenhuollon toimipisteessä saadakseen palvelua, sillä mobiilisovellus mahdollistaa potilaan tarkkailun myös sairaalan ulkopuolella. Terveydenhuollon ammattilaisen ei tarvitse olla kiinteän päätelaitteen ääressä vaan voi tarkastella potilaan tietoja mobiililaitteen kautta missä ja milloin vain. Terveydenhuollon etätoiminta on mahdollista potilaan luota löytyvällä laitteistolla. Etätoimintaa tukevia teknologioita ovat ainakin langattomat ja kaikkialla läsnäolevat kommunikaatiokanavat, nopeat datayhteydet, interaktiivinen video, robotiikka ja kosketusaistiin liittyvät teknologiat. (18)

Esimerkkejä mobiilista terveydenhuollosta on useita. Mobiilisovelluksilla voidaan jo nyt esimerkiksi kuntouttaa sepelvaltimotautipotilaiden sydäntä kotona (22) ja tarkkailla jatkuvasti iskemian tai rytmihäiriöiden alkumerkkejä (23). Yksityishenkilöt voivat pitää kirjaa fyysisistä aktiviteeteistaan (24) ja sydän- ja verisuonitautia tai diabetesta sairastavat voivat valvoa terveyteensä liittyviä fysiologisia tapahtumia valvonta- ja mobiililaitteen avulla (25). Android ja IOS käyttöjärjestelmien sovelluskaupoista löytyy lukuisia sovelluksia esimerkiksi painon pudotukseen ja terveellisten elämäntapojen ylläpitämiseen (26; 27; 28; 29; 30; 31; 32; 33; 34; 35; 36; 37). Osa näistä on käyttöjärjestelmän valmistajien kehittämiä (8; 9).

Tietoturva on olennainen vaatimus mobiilille terveydenhuollon järjestelmälle. Monet potilaat ovat huolissaan tietojen yksityisyyden säilymiestä, kun heidän henkilökohtaisia tietojaan lähetetään langattomien kanavien yli. Ajantasainen tarkkailu ja tietojen lähetys voi asettaa potilaan tiedot haitallisten tahojen tai salakuuntelijoiden saavutettaviin. Jos järjestelmän tiedonsiirron turvallisuudesta ei huolehdita, voi luvaton taho päästä käsiksi potilaan tietoihin ja muokata tai lisätä sinne väärää tietoa. (18) Ongelmana ei ole vain potilaan yksityisyyden menetys. Pahimmassa tapauksessa se voi altistaa potilaan hengenvaaraan esimerkiksi vääriksi vaihdettujen lääkeannostuksien kohdalla (17). Turvallisilla terveydenhuollon sovelluksilla on suuret vaatimukset langattomille ja mobiileille verkoille (18).

Yksi mobiilin terveydenhuollon tärkeistä osista ovat puettavat lääketieteelliset laitteet. Puettava lääketieteellinen laite on pieni, kevyt ja funktionaalinen laite, joka on kiinnitetty

ihmisen kehoon tai vaatetukseen. Se suorittaa ennalta määriteltyä lääketieteellistä tehtävää ja on tarvittaessa yhteistyössä muiden verkossa olevien laitteiden kanssa. Laitetta on helppo käyttää ja pitää yllä, eikä se häiritse käyttäjää. Tyypilliesti laite on rakennettu keskeisen prosessointiyksikön ympärille, sisältää oman voimalähteen ja on itsehallinnollinen. Sillä voidaan suorittaa fysiologista valvontaa, tiedon prosessointia ja etähoitoa siihen yhdistetyn mikroelektroniikan avulla. Prosessoitava tieto voi tulla käyttäjältä, laitteen sensoreilta tai ulkoiselta palvelimelta ja siitä prosessoitua palautetta voi tarkastella käyttäjä itse tai jokin toinen komponentti. Palautetta voidaan käyttää seurantaan, varoituksena tai päätösten teon tukena ja sen muoto voi olla visuaalinen, ääni, mekaaninen tai toisen laitteen toiminta. (21)

Puettavien laitteiden suosio on kasvussa ja niillä on potentiaalia tulla olennaiseksi osaksi modernia terveydenhuoltoa. Ne tarjoavat vaihtoehtoisia ratkaisuja suureen määrään lääketieteellisiä ja sosiaalisia tarpeita. Tämän lisäksi ne säästävät rahaa. Potilaiden sairaalaan joutuminen vähenee ennaltaehkäisyn ja itsenäisen asumisen tukemisen ansiosta. Osa puettavista laitteista käyttää hyväkseen älypuhelimen tuomia ominaisuuksia. Puhelimet ovat jo laajasti käytössä, joten niiden hyödyntäminen auttaa puettavien laitteiden käyttöönotossa (19; 21). Käyttämällä hyväksi puhelimista löytyvää teknologiaa saadaan puettavista laitteista yksinkertaisempia ja halvempia tuottaa (21).

Mahdollisia tehtäviä, joita puettavat laitteet voivat suorittaa, on useita. Näitä ovat muun muassa usean signaalin valvonta, hälytysmekanismit ja kaukotoimet. Sensoritekniikan ja biologisten signaalien analysoinnin kehittyminen on mahdollistanut sydämen, hengityksen, ihon lämpötilan, pulssin, verenpaineen ja veren happisaturaation tarkkailun. Muita tarkkailtavia asioita ovat kehon kinetiikka, aistit, sekä tunneperäinen ja kognitiivinen reaktiokyky. Eritoten potilaisiin liittyvät tehtävät, kuten hoidon tarjoaminen kohteessa, etätarkkailun mahdollistaminen, potilaan tilanteen seuraaminen samalla kun potilaalla on mahdollisuus liikkua ja potilaiden, kroonisesti sairaiden ja vammaisten kuntoutus ovat puettaville laitteille soveltuvia tehtäviä. Toinen tapa käyttää puettavia laitteita on lääkäreiden työkaluina. Tällöin laitteita voidaan käyttää esimerkiksi potilaiden tarkkailuun leikkauksessa tai elektronisen potilastietokannan ylläpitämiseen. Kolmas erilainen kohdeyleisö puettaville laitteille ovat terveet yksilöt. He voivat käyttää laitteita esimerkiksi terveyden tarkkailuun tai kuntoiluavustajina. (21) Yhdistämällä useita puettavia laitteita voidaan luoda kehosensoriverkko (*body sensor network, BSN*) (18). Kehosensoriverkon avulla voidaan tarkkailla henkilön terveyttä kokonaisvaltaisesti.

3.2 Terveydenhuollon lait ja säädökset

Potilaan etua valvotaan tiukalla alan sääntelyllä ja ankaralla viranomaisvalvonnalla (4). ”Lakisääteisten vaatimusten hallinta voi olla yritykselle joko kilpailuetu tai kaupaneste riippuen siitä, onko yritys itse ottanut riittävästi selvää vaatimuksista ja omaksunut ne omaan toimintaansa” (4). Näiden eritysvaatimusten hallinta on tärkeä kilpailutekijä myös tulevaisuudessa. Tekesin tekemän tutkimuksen mukaan sääntely ja säädöksiin liittyvät

vaatimukset ovat yksi suurimmista haasteista terveydenhuoltoon liittyvälle yritykselle. Erityisesti muutokset lainsäädännössä ja standardeissa, sekä tilanteet, joissa tuotetta ollaan viemässä uusille markkinoille tai ollaan CE-merkitsemässä. Säädökset kannattaa huomioida alusta alkaen. Tämä nopeuttaa markkinoille pääsyä ja vähentää ongelmatilanteita, joiden seurauksena pitää siirtyä aikaisempaan kehitysvaiheeseen. (4; 5)

Tässä työssä keskitytään vain Suomen ja Euroopan alueen lakeihin ja säädöksiin. Muun maailman säännöt eroavat näistä ja yrityksen tulee opetella jokaisen kohdemaan säännöt, joissa aikoo toimia. Euroopan unionin direktiiveissä määritellään lääkinnällisen laitteen ominaisuudet, luokittelu ja vaatimukset. Direktiivien vaatimukset ovat toteutettu Suomen laissa. Laki määrittää lisäksi vaatimuksia terveydenhuoltoon liittyvän tiedon käsittelyyn, poistamiseen, luovutuksen ja tarkastelijan lokitietojen keräämiseen. (38; 39; 40; 41; 42; 43) Suomessa terveydenhuollon laitteiden ja tarvikkeiden asianmukaisuutta valvoo Sosiaali- ja terveysalan lupa- ja valvontavirasto, Valvira (4; 44; 45).

Jotta lääkinnällinen laite voidaan tuoda markkinoille Suomen alueella, on siinä oltava CE-merkintä. CE-merkinnän liittämiseksi valmistajan on oltava tietoinen laitteeseen liittyvistä direktiiveistä ja standardeista, laitteen tulee täyttää siihen liittyvät vaatimukset, laitteelle on suoritettava kliininen arviointi, laite on testattava, laitteesta on luotava tarvittavat asiakirjat ja ilmoitukset, valmistajan on annettava vaatimustenmukaisuusvakuutus ja laite on rekisteröitävä Valviran ylläpitämään laiterekisteriin. Markkinoille tuomisen jälkeen valmistajan on valvottava laitteen toimintaa, sekä ilmoittaa Valviralle esimerkiksi laitteen aiheuttamista vaaratilanteista. Suuremman riskiluokan laitteille tulee olla käytössä myös laadunhallintajärjestelmä. (46; 47; 48; 49; 50) Laadunhallintajärjestelmä on sarja yritykseen kohdistuvia menettelyjä ja suunnitelmia. Sen avulla määritetään, miten tuote valmistetaan ja kuinka sen ympärillä oleviin asioihin reagoidaan.

Euroopan unionin vaatimukset lääkinnällisille laitteille tulee pääasiallisesti kolmen direktiivin kautta. Ne ovat direktiivi 90/385/ETY aktiivisia implementoitavia lääkinnällisiä laitteita koskevan jäsenvaltioiden lainsäädännön lähentämisestä, direktiivi 93/42/ETY lääkinnällisitä laitteista ja direktiivi 98/79/EY in vitro –diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista. Laki terveydenhuollon laitteista ja tarvikkeista (629/2010) toteuttaa nämä direktiivit Suomen lainsäädännössä. (51; 52; 53; 54; 55) ”Lain tarkoituksena on ylläpitää ja edistää terveydenhuollon laitteiden ja tarvikkeiden sekä niiden käytön turvallisuutta.” (51) ”Lakia sovelletaan terveydenhuollon laitteiden ja tarvikkeiden ja niiden lisälaitteiden suunnitteluun ja valmistukseen sekä toimenpidepakkausten ja järjestelmien kokoamiseen. Lisäksi lakia sovelletaan mainittujen tuotteiden markkinoille saattamiseen ja sitä varten steriloimiseen, käyttöönottoon, asennukseen, huoltoon, ammattimaiseen käyttöön, markkinointiin ja jakeluun.” (51)

3.2.1 Lääkinnälliset laitteet

Laitteen käyttötarkoitus määrittää paljolti sen onko laite terveydenhuollon laite vai ei. Valmistaja voi vaikuttaa laitteen luokitukseen ja siihen kohdistuviin vaatimuksiin käyttötarkoituksen määrityksellä. Oikeaa käyttötarkoitusta ei kuitenkaan voi kiertää, jos laitteen ominaisuudet määrittelevät sen selvästi terveydenhuollon laitteeksi. (4; 5; 51; 53; 56) Terveydenhuollon laitteen määritelmä on seuraava:

Instrumentti, laitteisto, väline, ohjelmisto, materiaali tai muu yksinään tai yhdistelmänä käytettävä laite tai tarvike, jonka valmistaja on tarkoittanut käytettäväksi ihmisen:

- sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen
- vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin
- anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun
- hedelmöittymisen säätelyyn. (51)

Sovellus voi olla terveydenhuollon laite, jolloin siihen pätee terveydenhuoltoon liittyvät säädökset. ”Ohjelmisto on lähtökohtaisesti terveydenhuollon laite silloin, kun sitä käytetään yksin tai yhdessä muiden terveydenhuollon laitteiden kanssa hankkimaan tietoa fysiologisten tilojen, terveydentilan, sairauksien tai synnynnäisten epämuodostumien havaitsemiseksi, diagnosoimiseksi, valvomiseksi tai hoitamiseksi. Vaatimuksia sovelletaan myös terveydenhuollon laiteita ohjaaviin tai niiden toimintaan vaikuttaviin erillisiin ohjelmistoihin.” (57) Sovellus voi olla myös lääkinnällisen laitteen lisälaite (56). Itsenäinen sovellus lasketaan aktiiviseksi lääkinnälliseksi laitteeksi, jos sovelluksen valmistaja on tarkoittanut sitä käytettäväksi nimenomaan yhteen tai useampaan lääkinnälliseen tarkoitukseen (56; 58; 59).

Kaikkia terveydenhuollossa käytettyjä sovelluksia ei voida määritellä lääkinnällisiksi laitteiksi. Esimerkiksi sovellukset, jotka suorittavat vain yksinkertaisia hakuja, siirtävät dataa muuttamatta sitä tai luovat yleispäteviä diagnooseja väestötietoihin perustuen eivät ole lääkinnällisiä laitteita. Terveydenhuollossa käytettävän sovelluksen virhetoimintoon liittyvä riski ei ole peruste määritellä sovellusta lääkinnälliseksi laitteeksi. Sovellus voi toimia eri käyttöjärjestelmissä tai virtuaaliympäristöissä. Nämä käyttöjärjestelmät tai virtuaaliympäristöt eivät vaikuta määrittelyyn. (58; 56; 59)

In vitro –diagnostiikkaan tarkoitettu lääkinnällinen laite on reagenssi, reagenssituote, kalibraattori, vertailumateriaali, testipakkaus, instrumentti, laite, laitteisto tai järjestelmä joko yksin tai yhdessä muiden kanssa käytettynä ja jonka valmistaja on tarkoittanut käytettäväksi in vitro ihmiskehosta otettujen näytteiden, mukaan lukien veren ja kudosten luovutukset, tutkimisessa yksinomaisena tai pääasiallisena tarkoituksena saada tietoa fysiologisesta ja patologisesta tilasta, synnynnäisestä epämuodostumasta, turvallisuuden ja yhteensopivuuden määrittämiseksi mahdollisten saajien kannalta tai hoitotoimenpiteiden

tarkkailemiseksi. (53; 54) Itsenäinen sovellus on ”in vitro -diagnostiikkaan (IVD) tarkoitettu lääkinnällinen laite tai in vitro -diagnostiikkaan tarkoitetun lääkinnällisen laitteen lisälaite, jos se täyttää direktiivin 98/79/EY IVD-diagnostiikkaan tarkoitetun laitteen tai IVD-diagnostiikkaan tarkoitetun laitteen lisävarusteen määritelmän” (56).

3.2.2 Lääkinnällisten laitteiden luokitukset

Ei ole perusteltua, eikä taloudellisesti järkevää asettaa kaikille lääkinnällisille laitteille tiukimpia mahdollisia vaatimuksia. Tämän takia laitteet jaetaan eri luokkiin, joilla on omat vaatimustasot. Valmistajan on annettava laitteelle käyttötarkoitus ja määritettävä sen tuoteluokka ennen tuotteen saattamista markkinoille (4; 60). Jaottelu on tehty suoraan Euroopan unionin direktiivissä, jotta valmistajat tietävät laitteensa luokan mahdollisimman aikaisessa kehitysvaiheessa. Jaottelu perustuu riskeihin ja mahdolliseen haittaan, jota se voi luoda ihmiselle. (4; 53; 59; 61) Mitä suurempi mahdollisen haitan riski, sitä korkeampi luokka ja sitä enemmän vaaditaan tuotekehitykseltä ja tuotteen koko elinkaarelta (4).

Ominaisuuksia, jotka otetaan luokittelussa mukaan, ovat:

- Kesto. Laite tarkoitettu tavanomaisesti käytettäväksi yhtäjaksoisesti alle 60 minuuttia (tilapäinen), enintään 30 vuorokautta (lyhytaikainen) tai yli 30 vuorokautta (pitkäaikainen).
- Invasiivisuus. Laite viedään kokonaan tai osittain kehon sisään. Vienti tapahtuu kehon luonnollisten aukkojen kautta tai kirurgisella toimenpiteen avulla tai sen yhteydessä.
- Käytetään kirurgisiin toimenpiteisiin.
- Muun kuin ihmiskehosta saatavan voiman tai painovoiman käyttämistä energialähteenä.
- Aktiivisten lääkinnällisten laitteiden biologisten toimintojen tai rakenteiden ylläpito, muutto, korvaus tai korjaus sairauden, vamman tai haitan hoitamiseksi tai lievittämiseksi.
- Aktiivisten lääkinnällisten laitteiden tietojen hankkiminen fysiologisista tiloista, terveydentilasta, sairauksista tai synnynnäisistä epämuodostumista niiden havaitsemiseksi, diagnosoimiseksi, valvomiseksi tai hoitamiseksi.
- Keskusverenkierron kanssa tekemisissä oleminen.
- Keskushermoston kanssa tekemisissä oleminen. (53; 61)

Luokitussääntöjä sovelletaan laitteiden käyttötarkoituksen mukaisesti. Jos laite on tarkoitettu käytettäväksi muiden laitteiden kanssa, luokitussääntöjä sovelletaan erikseen kuhunkin laitteeseen. Lisälaitteet luokitellaan erillään laitteista, joiden kanssa niitä käytetään. Terveydenhuollon laitetta ohjaava tai sen toimintaan vaikuttava tietokoneohjelma kuuluu

samaan luokkaan, kuin ohjattava laite. Jos laitetta ei ole tarkoitettu käytettäväksi yksinomaan tai olennaisesti tiettyyn kehon osaan, se on luokiteltava tärkeimmän määritellyn käyttötarkoituksen mukaisesti. Jos samaan laitteeseen sovelletaan useampia sääntöjä, niistä valitaan tiukin. (4; 53)

Terveydenhuollon laitteet jaotellaan ominaisuuksiensa perusteella tuoteluokkiin I, II a, II b ja III. Luokan I laitteen vaatimustenmukaisuuden arvioinnin kannalta on soveltuvin osin lisäksi määritettävä, onko laitteessa mittaustoiminto (Im) ja onko laite steriili (Is). Luokan I vaatimukset ovat väljimmät ja luokan III tiukimmat. Luokan I laitteet ovat luokitelluista laitteista vähiten vaarallisia käyttäjälle. Ne vaikuttavat kehon ulkopuolella tai ovat sisäpuolella vain lyhyen ajan ja silloinkin luonnollisen aukon kautta. Luokka IIa ja IIb ovat laitteille, jotka ovat väärin toimiessaan luokan I laitteita vaarallisempia. Ne voivat olla kehon sisällä pitkiäkin aikoja luonnollisen aukon tai kirurgisen operaation kautta. Luokka III on laitteille, jotka toimiessaan väärin voivat luoda suurta vahinkoa käyttäjälle. Ne voivat vaikuttaa tärkeisiin elimiin ja olla käyttäjän sisällä kuolemaan saakka. Luokkaan I kuuluvia laitteita ovat muun muassa laitteet, jotka eivät ole kosketuksissa potilaan kanssa, ovat kosketuksissa rikkinäisen ihon kanssa, mutta vain luodakseen suojan, puristaakseen tai imeäkseen eritteitä, ovat hetkellisesti kehon sisällä luonnollisen aukon kautta ja uudelleenkäytettävät kirurgiset laitteet. Luokkaan II a kuuluvia laitteita ovat muun muassa laitteet, jotka ovat tarkoitettu hallitsemaan haavan mikroympäristöjä, ovat lyhytaikaisesti kehon sisällä luonnollisen aukon kautta, ovat hetkellisesti tai lyhytaikaisesti kehon sisällä kirurgisen toimenpiteen kautta ja ovat tarkoitettu lääkinnällisten laitteiden desinfektointiin. Luokkaan II b kuuluvia laitteita ovat muun muassa laitteet, jotka muokkaavat veren tai muun kehon nesteen biologista tai kemiallista koostumusta, ovat pitkäaikaisesti kehon sisällä luonnollisen aukon kautta, ovat hetkellisesti tai lyhytaikaisesti kehon sisällä kirurgisen toimenpiteen kautta tuottaakseen biologisen vaikutuksen, joka absorboidaan suurimmaksi osaksi tai kokonaan, ovat pitkäaikaisesti kehon sisällä kirurgisen toimenpiteen kautta tai laite on implantti ja ovat tarkoitettu ehkäisyyn tai sukupuolitautien torjumiseen. Luokkaan III kuuluvia laitteita ovat muun muassa laitteet, jotka ovat tarkoitettu hallinnoimaan, diagnosoimaan, tarkkailemaan tai korjaamaan virheitä sydämessä tai keskusverenkierrossa suoralla kosketuksella, ovat pitkäaikaisesti kehon sisällä kirurgisen toimenpiteen kautta tai laite on implantti pois lukien hampaissa olevat ja suorassa kosketuksessa keskushermoston kanssa olevat laitteet. (4) Yksityiskohtaisemmat ohjeet laitteen luokittelusta voi lukea Euroopan Unionin neuvoston direktiivistä 93/42/ETY (53).

In vitro -diagnostiikkaan tarkoitetut terveydenhuollon laitteet jaotellaan Euroopan parlamentin ja neuvoston direktiivistä 98/79/EY löytyviin luettelon A ja luettelon B laitteisiin, sekä niiden ulkopuolelle jääviin muihin laitteisiin. Ne jaetaan myös käyttötarkoituksen mukaan itse suoritettavaan testaukseen tarkoitettuihin laitteisiin, suorituskyvyn arviointiin tarkoitettuihin laitteisiin ja muihin laitteisiin. Laitteiden luokat määräytyvät MD- (*medical device*) ja IVD-direktiivien (*in vitro device, IVD*) perusteella. Luettelon A laitteita ovat reagenssit ja reagenssituotteet ABO-järjestelmän, Rhesus (C, c, D, E, e) ja anti-Kell

veriryhmien määritykseen, sekä HIV-infektion, HTLV I:n ja II:n, hepatiitti B:n, C:n ja D:n merkkiaineiden toteamiseen, vahvistamiseen ja määrän ilmaisemiseen ihmisestä otetuista näytteistä. Luettelon B laitteita ovat muun muassa reagenssit ja reagenssituotteet Anti-Duffy ja Anti-Kidd veriryhmien määrityksiin, tavallisuudesta poikkeavien punasolujen vastaisten vasta-aineiden määrityksiin ja sytomegaloviruksen tai klamydian toteamiseen. (4; 54)

Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira myös listaa aktiiviset implantit omana luokkanaan. Valvira voi antaa tarkempia määräyksiä laitteiden luokkien määräytymisestä. (51; 62) Itsenäiset sovellukset, jotka lasketaan aktiivisiksi lääkinnällisiksi laitteiksi, kuuluvat luokkaan I, jos niihin ei sovelleta jotain Euroopan Unionin direktiivin 93/42/EEC liitteen IX sääntöjä 9, 10 tai 11, jolloin ne kuuluvat joko luokkaan II a tai II b. Nämä säännöt käsittävät muun muassa energian tuottamisen, laitteiden tehon tarkastuksen tai valvonnan, diagnosoinnin, säteilyn lähettämisen ja lääkkeiden annostelun. (53; 56; 58) Itsenäisen sovelluksen on ensin täytettävä lääkinnällisen laitteen määritelmä, jotta se voidaan määritellä in vitro -diagnostiikkaan tarkoitetuksi lääkinnälliseksi laitteeksi. Tarkat määritelmät luokittelulle tulee lukea suoraan direktiiveistä.

Luokituksesta riippuen valmistajan tulee CE-merkinnän kiinnittämiseksi noudattaa eri menettelyjä. Menettelyjä on useita ja monet niistä ovat vaihtoehtoisia toistensa kanssa. Valmistaja voi itse valita vaihtoehdoista sen menettelyn, jolla haluaa arvioida tuotteen vaatimustenmukaisuuden. Luokan III laitteet esimerkiksi vaativat joko täydellisen laadunvarmistusjärjestelmän mukaisen EY-vaatimustenmukaisuusvakuutusmenetelmän noudattamista tai EY-tyyppitarkastuksen ja EY-tarkastuksen tai tuotannon laadunvarmistuksen mukaisen EY-vaatimustenmukaisuusvakuutusmenettelyjen yhdistelmän noudattamista. Luokkiin liittyviä menettelyjä ei ole listattu tähän, sillä ne löytyvät helposti Valviran terveydenhuollon laitteen ja tarvikkeen vaatimustenmukaisuuden arviointimääräyksestä. (63)

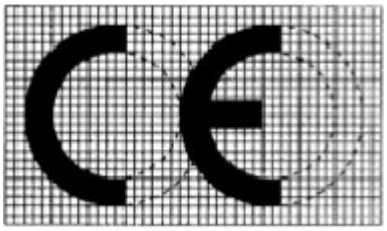
3.2.3 Vaatimustenmukaisuusvakuutus ja CE-merkintä

Valmistajan on annettava laitteelle, lukuun ottamatta yksilölliseen käyttöön valmistettuja ja kliinisiin tutkimuksiin tarkoitettuja laitteita, vaatimustenmukaisuusvakuutus, ennen kuin se voidaan saattaa markkinoille Euroopan unionin talousalueella. Vaatimuksenmukaisuusvakuutuksen antamiseksi laitteen on täytettävä sille laeissa ja direktiiveissä asetetut vaatimukset, laitteelle tulee suorittaa kliininen arviointi, laite tulee testata, siitä tulee luoda tarvittavat asiakirjat ja ilmoitukset ja se tulee rekisteröidä Valviran ylläpitämään laiterekisteriin. Laadunhallintajärjestelmän käyttö on pakollista suuremman riskiluokan laitteille, mutta suositeltavaa kaikille laitteille luokasta riippumatta. Tom Ståhlberg kirjoittaa ”Terveydenhuollon lakisääteiset määräykset kansanvälisillä markkinoilla” oppaassa, että vaatimuksia ei käytännössä pysty saavuttamaan ollenkaan ilman toimivan laadunhallintajärjestelmän käyttöä. (4; 46; 47; 48; 49; 50)

Vaatimukset käsittävät suunnittelun, valmistuksen ja laitteen kaikkien osien koko elinkaaren. Yleisesti tämä menettely takaa, että laite on Euroopan neuvoston asettamien olennaisten vaatimusten mukainen, ei vaaranna potilaan, käyttäjän tai kenenkään muun henkilön terveyttä, turvallisuutta tai ympäristöä, sekä oikeasti käytettynä laite saavuttaa sille asetetun toimivuuden ja suorituskyvyn. Valmistajan tulee pystyä todistamaan teknisillä asiakirjoilla ja dokumenteilla, että laite täyttää nämä vaatimukset. Vaatimusten täyttäminen onnistuu laitteelle määrättyjä standardeja noudattamalla. Standardien noudattaminen on vapaaehtoista, jos vaatimukset täytetään muilla teknisillä ratkaisuilla. (4; 5; 51; 53)

Kun valmistaja on varma, että laite täyttää vaatimukset, hän allekirjoittaa laitteesta EU-vaatimustenmukaisuusvakuutuksen ja varustaa laitteen CE-vaatimustenmukaisuusmerkinnällä (*Conformité Européenne, CE*) (4; 49; 51; 53). Merkintä on oltava riippumatta laitteen valmistusmaasta (49). Jos laite ei täytä sille osoitettuja vaatimuksia, CE-merkintää ei saa kiinnittää (49; 51; 53). Laitteen valmistaja on yksin vastuussa siitä, että laite on kaikkien vaatimusten mukainen. Todistaakseen CE-merkinnän olevan oikeutettu valmistaja saattaa joutua toimittamaan asiakirjat maahantuojille tai jakelijoille. (49) ”CE -merkintä on kiinnitettävä näkyvällä, helposti luettavalla ja pysyvällä tavalla laitteeseen tai steriiliin pakkaukseen. Tarvittaessa merkintä ilmoitetaan myös käyttöohjeissa ja myyntipakkauksessa. Mikäli vaatimustenmukaisuuden arviointimenettelyjen täytäntöönpanossa on käytetty ilmoitettua laitosta, CE -merkintään liitetään laitoksen tunnusnumero.” (64)

CE-vaatimustenmukaisuusmerkintä koostuu kirjaimista ”CE” kuvan 1 tavalla kirjoitettuna. Mittasuhteita on noudatettava, jos merkinnän koko muutetaan. Kirjainten on oltava saman korkuisia ja vähintään 5 mm korkeita. Pienemmissä laitteissa koko voi olla vielä pienempi. (53) ” Laitteeseen ei saa kiinnittää sellaisia merkintöjä, jotka muistuttavat CE -merkintää. Laitteeseen, pakkaukseen tai laitteen mukana seuraavaan ohjeeseen voidaan kiinnittää muita merkkejä, jos ne eivät heikennä CE -merkinnän näkyvyyttä ja luettavuutta.” (64) Yksilölliseen käyttöön, kliinisiin tutkimuksiin tai suorituskyvyn arviointiin tarkoitettuja laitteita ei varusteta CE -merkinnällä. (53; 65)



Kuva 1. CE-merkintä (53)

Oikeilla perusteilla kiinnitetty CE-merkintä varmistaa, että jäsenvaltiot eivät estä tuotteen saattamista markkinoille tai ottamasta sitä käyttöön alueellaan. Perusteettomasti kiinnitetystä CE-merkinnästä jäsenvaltiot ovat velvolliset tekemään kaikki aiheelliset toimenpiteet kyseisen tuotteen markkinoille saattamisen rajoittamiseksi tai kieltämiseksi ja sen

varmistamiseksi, että se vedetään markkinoilta. (53) Suomessa terveydenhuoltoon liittyviä säädöksiä valvoo Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira ja aluehallintovirasto. (57; 66) Valvira voi antaa tarkempia määräyksiä CE-merkintöjen käytöstä terveydenhuollon laitteissa (51).

3.2.4 Olennaiset vaatimukset

Terveydenhuollon laitteen tulee täyttää sitä koskevat olennaiset vaatimukset. Laite täyttää olennaiset vaatimukset silloin, kun se on suunniteltu, valmistettu ja varustettu sitä koskevien kansallisten standardien mukaisesti. (49; 51; 67) Kokonainen lista vaatimuksista löytyy kunkin Euroopan unionin neuvoston direktiivin liitteestä I. Vaatimukset jakaantuvat yleisiin vaatimuksiin ja suunnittelua ja rakennetta koskeviin vaatimuksiin. Tässä luvussa käymme läpi joitain vaatimuksista, jotka saattavat liittyä terveydenhuollon mobiilisovelluksiin. Listan muita vaatimuksia ei käsitellä tässä työssä. Valmistajan on kuitenkin hyvä lukea koko lista läpi varmistuakseen omaan tuotteeseen liittyvistä vaatimuksista. (53)

”Laitteen tulee olla käyttötarkoitukseensa sopiva ja sen tulee käyttötarkoituksensa mukaisesti käytettynä saavuttaa sille suunniteltu toimivuus ja suorituskyky. Laitteen asianmukainen käyttö ei saa tarpeettomasti vaarantaa potilaan, käyttäjän tai muun henkilön terveyttä tai turvallisuutta.” (51) Jos laite on ohjelmisto tai sisältää ohjelmiston on kyseinen ohjelmisto validoitava parhaiden käytäntöjen mukaisesti ottaen huomioon kehityskaareen, riskinhallintaan, validointiin ja tarkastuksiin liittyvät periaatteet. Laitteen mukana on oltava laitteen turvalliseen ja asianmukaiseen käyttöön tarvittavat tiedot. Käyttöohje on oltava jokaisessa laitteen pakkauksessa pois lukien I ja II a luokan laitteet, jos niitä voidaan käyttää turvallisesti ilman ohjeiden apua. Ohjeiden sisältämiin tietoihin löytyy useita vaatimuksia, jotka valmistajan tulee täyttää. Aineita, kuten lääkkeitä tai vastaavia, kuljettaville laitteille on erillisiä vaatimuksia. Nämä voivat myös liittyä mobiililaitteen sovelluksien vaatimuksiin. Esimerkiksi sovelluksen, joka vastaa annostelun oikean määrän varmistamisesta tai vaarallisista aineista käyttäjän varoittamisesta, on täytettävä nämä vaatimukset. (53) Valvira voi antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä (51).

3.2.5 Suomen lain määrittämät lisävaatimukset

Suomen lait toteuttavat Euroopan unionin direktiivien vaatimukset, mutta määrittävät myös omia vaatimuksia terveydenhuoltoon liittyville sovelluksille. Suuri osa näistä vaatimuksista on säädetty laissa ”Laki terveydenhuollon laitteista ja tarvikkeista”. Tässä luvussa keskistytään tähän lakiin terveydenhuollon mobiilisovelluksen kehittämisen näkökulmasta. Jos sovellukseen tai laitteeseen, jossa sovellus toimii, liittyy erityisominaisuuksia, niin valmistajan tulee toteuttaa myös näihin ominaisuuksiin liittyvien lakien vaatimukset. (51)

Valmistajan on tehtävä terveydenhuollon laitetta markkinoille saatettaessa sekä aloitettaessa palvelun tuottaminen Valviralle ”ilmoitus, josta käy selville valmistajan ja tarvittaessa valtuutetun edustajan nimi, toimipaikka, laitteen käyttötarkoitus, toimintaperiaate ja sellaiset tiedot, joiden avulla laite voidaan tunnistaa. Terveydenhuollon laitteesta, joka voi aiheuttaa merkittävän terveydellisen riskin, on lisäksi ilmoitettava tiedot merkinnöistä ja käyttöohjeista.” (51)

”Valmistajan on annettava terveydenhuollon laitteen yhteydessä turvallisuuden kannalta tarpeelliset tiedot sen käytöstä, varastoinnista ja kuljettamisesta.” (51) ”Laitteen mukana olevien tietojen on oltava suomen, ruotsin tai englannin kielellä, jollei tietoja ole annettu yleisesti tunnetuilla ohje- tai varoitusmerkinnöillä. Käyttäjälle tai potilaalle tarkoitettujen, laitteen turvallisen käytön edellyttämien tietojen on kuitenkin oltava suomen ja ruotsin kielellä. Valmistajan on riskianalyysin perusteella määriteltävä, mitkä ovat turvallisen käytön edellyttämiä tietoja. Itse suoritettavaan testaukseen tarkoitettujen laitteiden sekä yksilölliseen käyttöön valmistettujen laitteiden käyttöohjeiden ja merkintöjen on oltava suomeksi ja ruotsiksi.” (51; 68) ”Terveydenhuollon laitteen markkinointi, johon sisältyy myös mainonta ja muu myynninedistämistoiminta, ei saa olla epäasiallista eikä se saa antaa liioiteltua tai virheellistä kuvaa laitteesta tai sen vaikuttavuudesta tai käytöstä” (51).

”Valmistajan on seurattava ja arvioitava ajantasaisella järjestelmällisellä menettelyllä terveydenhuollon laitteista tuotannon jälkeen saatavia kokemuksia sekä laitteen kliiniseen arviointiin liittyviä tietoja” (51). ”Valmistajan on säilytettävä vaatimustenmukaisuutta koskevat ja muut valvonnan edellyttämät tiedot vähintään viiden vuoden ajan terveydenhuollon laitteen valmistuksen päättymisestä tai kliinisiin tutkimuksiin, suorituskyvyn arviointiin ja yksilölliseen käyttöön tarkoitetun laitteen valmistumisesta. Implantoitavia laitteita koskevien tietojen säilytysaika on kuitenkin vähintään 15 vuotta.” (51) Valmistajan on ilmoitettava Valviralle tilanteista, jotka ovat johtaneet tai olisivat saattaneet johtaa potilaan, käyttäjän tai muun henkilön terveyden vaarantumiseen, ja jotka johtuvat terveydenhuollon laitteen ominaisuuksista, suorituskyvyn poikkeamasta tai häiriöstä, riittämättömästä merkinnästä tai riittämättömästä tai virheellisestä käyttöohjeesta. Valmistajan on myös ilmoitettava Valviralle kaikki terveydenhuollon laitteen ominaisuuksiin ja suorituskykyyn liittyvät edellä mainituista seikoista johtuvat tekniset ja lääketieteelliset syyt, joiden vuoksi valmistaja järjestelmällisesti poistaa samaa tyyppiä olevat laitteet markkinoilta. (51)

Asiakastietojen käsittelyyn terveydenhuollon alalla on erillisiä sääntöjä. Nämä säännöt löytyvät laista ”Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä”. Lain tarkoitus on ”edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä” (43) ja toteuttaa ”yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi”. (43)

”Asiakastietojen sähköisessä käsittelyssä tulee turvata tietojen saatavuus ja käytettävyys. Asiakastietojen tulee säilyä eheinä ja muuttumattomina koko niiden säilytysajan” (43). ”Sähköisestä asiakasasiakirjasta tulee olla vain yksi alkuperäinen tunnisteella yksilöity kappale. Alkuperäisestä asiakirjasta voidaan palvelun toteuttamiseksi tai muusta perustellusta syystä ottaa jäljennös, josta tulee ilmetä asiakirjan olevan jäljennös.” (43) ”Sosiaalihuollon ja terveydenhuollon palvelujen antajan tulee pitää rekisteriä omien asiakastietojärjestelmiensä ja asiakasrekisteriensä käyttäjistä sekä näiden käyttöoikeuksista.” (43) ”Palvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojen käytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin. Käyttölokirekisteriin tallennetaan tieto käytetyistä asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja käytetään, asiakastietojen käyttäjästä, tietojen käyttötarkoituksesta ja käyttöajankohdasta. Luovutuslokirekisteriin tallennetaan tieto luovutetuista asiakastiedoista, siitä palvelujen antajasta, jonka asiakastietoja luovutetaan, asiakastietojen luovuttajasta, tietojen luovutustarkoituksesta, luovutuksensaajasta ja luovutusajankohdasta.” (43) Kansaneläkelaitoksen tulee kerätä vastaavat tiedot potilaan tiedonhallintapalveluun tallennettujen ja sen kautta näytettyjen tietojen luovuttamisesta (43). ”Asiakastietojen käyttäjien käyttöoikeustiedot ja lokitiedot tulee hävittää, kun ne eivät enää ole tarpeen asiakastietojen käytön ja luovutuksen lainmukaisuuden seuraamiseksi” (43).

Terveydenhuollon potilastietojärjestelmien ja potilasasiakirjojen tietorakenteiden tulee mahdollistaa sähköisten potilasasiakirjojen käyttö, luovuttaminen, säilyttäminen ja suojaaminen valtakunnallisten tietojärjestelmäpalvelujen avulla. ”Terveydenhuollon palvelujen antajan tulee luokitella erityistä suojausta edellyttävät potilasasiakirjat ja potilastiedot erillisellä vahvistuspyynnöllä suojattaviin potilastietoihin.” (43) ”Asiakastietojärjestelmästä tulee voida tuottaa sosiaalihuollon ja terveydenhuollon palvelujen antajan oman suunnittelun, johtamisen ja tilastoinnin, sekä valtakunnallisen tutkimus- ja tilastotoiminnan kannalta tarpeelliset tiedot ja hoidon tarpeen arviointia sekä hoitoon pääsyn ajankohtaa koskevat tiedot.” (43)

”Asiakastietojen sähköisessä käsittelyssä asiakas, sosiaalihuollon ja terveydenhuollon palvelujen antaja, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet tulee tunnistaa luotettavasti. Potilastietoja käsittelevien henkilöiden, palvelujen antajien, tietoteknisten laitteiden sekä valtakunnallisten tietojärjestelmäpalvelujen tunnistaminen edellyttää lisäksi todentamista.” (43) ”Asiakastietojen eheys, muuttumattomuus ja kiistämättömyys tulee varmistaa sähköisellä allekirjoituksella tietojen sähköisessä käsittelyssä, tiedonsiirrossa ja säilytyksessä. Luonnollisen henkilön sähköisessä allekirjoittamisessa tulee käyttää kehittynyttä sähköistä allekirjoitusta.” (43)

3.2.6 Kliininen arviointi, laitetutkimus ja ilmoitettu laitos

Terveydenhuollon laitteelle tulee aina tehdä kliininen arviointi ennen markkinoille saattamista. Kliininen arviointi on valmistajan kliinisten tietojen perusteella tekemä arviointi,

jossa tutkitaan terveydenhuollon laitteen ja tarvikkeen toimivuutta ja käyttöön soveltuvuutta. Arvioinnissa käsitellään laitteen ominaisuuksia, suorituskykyä ja haittavaikutuksia ja otetaan kantaa sivuvaikutusten haittahyötysuhteen hyväksyttävyyteen. Arvioinnin tietojen on oltava peräisin joko laitetta tai samankaltaista laitetta koskevasta kliinisestä laitetutkimuksesta tai raportista. (4; 51; 69; 70)

Kliininen laitetutkimus on ”ihmisiin kohdistuva tutkimus, joka tehdään terveydenhuollon laitteen ja tarvikkeen käyttötarkoituksen ja ominaisuuksien määrittämiseksi, arvioimiseksi tai tarkistamiseksi.” (70) Implantoitavalla ja III tuoteluokan laitteille tulee tehdä kliininen laitetutkimus, ellei ole perusteltua syytä nojautua olemassa oleviin aiempiin kliinisiin tietoihin. ”Kliinisestä laitetutkimuksesta vastaavan henkilön tulee olla lääkäri tai hammaslääkäri, jolla on asianmukainen ammatillinen ja tieteellinen pätevyys.” (70) Tutkimuksen suunnittelun ja toteuttamisen apuna voidaan käyttää standardia SFS-EN ISO 14155. Tutkimuksen aloittamisesta tulee ilmoittaa Valviralle. Lomake ilmoitukseen löytyy Valviran sivuilta. Ilmoituksen käsittely on maksullinen ja se on jätettävä ennen tutkimuksen aloittamista. Korkeamman tuoteluokan laitteille vaaditaan, että ilmoitus on jätetty 60 vuorokautta ennen aloitusta. (4; 51; 69; 70) ”Toimeksiantajan on annettava selvitys tutkimuksen tuloksista Valviralle mahdollisimman pian ja viimeistään yhden vuoden kuluttua tutkimuksen päättymisestä” (70). ”Tutkimuksen aikana todetut vakavat vaaratilanteet on toimeksiantajan välittömästi ilmoitettava Valviralle” (70). ”Tutkimukseen liittyviä selvityksiä on Valviran kehotuksesta annettava myös tutkimuksen aikana” (70).

Joissain tapauksissa ei riitä, että valmistaja itse arvioi laitteen, vaan arviointi tulee teettää puolueettoman kolmannen osapuolen ilmoitetulla laitoksella (*notified body*). Ilmoitettua laitosta tulee käyttää tuoteluokkien IIa, IIb ja III lääkinnällisten laitteiden arvioinnissa, tuoteluokan I steriilin tai mittaustoiminnon omaavan laitteen steriiliyden tai mittaustoiminnon arvioinnissa ja IVD-laitteiden arvioinnissa, jos ne ovat luettelossa A tai B. Tuotteen tulee kuulua ilmoitetun laitoksen pätevyysalueelle. Ilmoitetut laitokset ovat Euroopan unionin jäsenvaltioiden nimeämiä. Niitä valvoo kunkin maan toimivaltainen viranomainen. Suomessa sijaitsevia lääkinnällisiä laitteita arvioivia ilmoitettuja laitoksia on kaksi, SGS Fimko Oy ja VTT Expert Services Oy. Luettelo ilmoitetuista laitoksista ja niiden pätevyysalueista löytyy Euroopan unionin komission ylläpitämästä NANDO-rekisteristä (*new approach notified and designated organisations*). Valmistaja voi käyttää minkä tahansa jäsenvaltion ilmoitettua laitosta, mutta oman maan laitoksen käyttäminen on yleensä kätevämpää yhteisen kielen, kulttuurin, aika- ja/tai kustannustehokkuuden takia. (4; 50; 71; 72) Jos ilmoitetun laitoksen käyttämistä vaaditaan, on valmistajan jätettävä ilmoitetulle laitokselle suunnitteluasiakirjoja koskeva tutkimuspyyntö laitteesta. Pyynnössä on kuvailtava kyseisen laitteen suunnittelu, valmistus ja suorituskyky ja oltava mukana tarvittavat asiakirjat. Ilmoitettu laitos voi vaatia täydennystä pyyntöön. Jos laite on säännösten mukainen, ilmoitettu laitos antaa hakijalle EY-suunnittelutarkastustodistuk-

sen. Ilmoitettu laitos voi tehdä valmistajan toimitiloihin yllätyskäyntejä ja suorittaa testejä. (53) CE-merkintään liitetään laitoksen tunnusnumero, jos vaatimustenmukaisuuden arviointimenettelyjen täytäntöönpanossa on käytetty ilmoitettua laitosta. (53; 64)

4. MOBIILISOVELLUSTEN KEHITYS

Mobiilisovellusten kehitys eroaa muiden ohjelmien kehityksestä erinäisin tavoin. Mobiilisovellusten alustat, teknologiat ja jakelukanavat ovat omanlaisensa. Mobiililaitteet alustana mahdollistavat monenlaisten eri ominaisuuksien käytön, joita muista laitteista ei välttämättä löydy, mutta rajoittavat myös sovellusta pienen koon, kommunikaatioväylien ja laitteen tehojen takia. Tässä luvussa käydään läpi mobiilisovellusten kehitykseen liittyvät asiat. Luvussa esitellään mobiilisovelluksien suurimmat käyttöjärjestelmät, teknologiat ja jakelukanavat, sekä vertaillaan niitä. Myöhemmin käymme läpi mobiilikehityksen yleiset haasteet ja mitä erityistä pitää ottaa huomioon, kun mietitään mobiilisovellusten tietoturvaa.

4.1 Käyttöjärjestelmät

Tämän hetken kaksi suurinta mobiilikäyttöjärjestelmää ovat Applen iOS ja Googlen Android (73). Sovelluksia voidaan kehittää myös muille alustoille, mutta tässä työssä keskitytään näihin kahteen. Mobiilisovellusten kehitykseen iOS ja Android käyttöjärjestelmille tarvitaan yleisesti työkalut, ohjelmointikielten osaamista ja kehitystunnukset. Tässä luvussa käydään läpi tarkasti mitä näille alustoille kehittäminen vaatii ja mitä alustalle suunnatut kehitysresurssit mahdollistavat.

4.1.1 iOS

Kehitys iOS käyttöjärjestelmälle tapahtuu Applen tarjoamilla työkaluilla. Nämä työkalut toimivat suoraan vain Applen tuotteissa. Apple tarjoaa työkalut ja resurssit sovellusten kehitykseen ilmaiseksi, mutta kehittäjätunnukset maksavat 99 Yhdysvaltojen dollaria per vuosi. Kehittäjätunnukset tarvitaan, jos haluaa julkaista sovelluksen App Store sovelluskaupassa. App Store on Applen sovelluskauppa. (74; 75)

Kehitystunnuksien kautta kehittäjä saa myös ladattua uusimmat betaversiot käyttöjärjestelmistä, käyttöönsä Applen analytiikkatyökaluja ja mahdollisuuden käyttää Applen teknistä tukea kahdesti ilman erillistä maksua. Betaversioiden avulla kehittäjä voi varautua mahdollisiin muutoksiin ja tekemään tarvittavat muutokset sovelluksiin etukäteen. Teknisen tuen avulla kehittäjä voi ratkaista kooditason ongelmia. Analytiikkatyökalut kertovat tietoja sovellusta tarkastelevista ihmisistä. Esimerkiksi miten ihmiset löytävät sovelluksen ja mitkä asiat vaikuttivat sen lataamiseen. Tietojen avulla sovelluksen kehitystä voidaan paremmin suunnitella vastaamaan käyttäjien haluja. Sovelluksen testaaminen tapahtuu myös kehitystunnusten kautta. Enimmäismäärä testaajia on 10 000 henkilöä. Julkaisun jälkeen kehittäjä voi antaa rajallisen määrän käyttäjiä ladata sovelluksen ilmaiseksi App Storesta testattavaksi. Tällaisten käyttäjien määrä on sata joka laitetyypille vuodessa.

(74; 76) Ilman kehitystunnuksia sovelluksen pystyy lataamaan omaan laitteeseen, mutta sovelluksen kykyä käyttää Applen palveluja on rajoitettu. (77)

4.1.2 Android

Google tarjoaa ohjelmien kehityspaketin ilmaiseksi. Kehittäjätunnukset maksavat 25 Yhdysvaltojen dollaria ja ne ovat voimassa ikuisesti. Tunnukset tarvitaan Play Console sivuston käyttämiseen ja sovelluksen julkaisemiseen Google Play sovelluskaupassa. Google Play on Googlen sovelluskauppa. (78) Play Console sivusto, jonka kautta voidaan hallinnoida ja päivittää sovellus. Sieltä löytyy myös paljon erilaista statistiikkaa sovelluksesta. Sovelluksen voi laittaa testattavaksi pienelle tai suurelle joukolle testaajia. Suljettuun testaukseen voidaan valita 50 käyttäjälistaa ja jokaisella listalla voi olla enintään 2000 käyttäjää. Suljettuun testaukseen voidaan kutsua siis enintään 100 000 käyttäjää. Käyttäjälistoja voidaan uudelleen käyttää muissa testauksissa. Käyttäjät listataan sähköpostiosoitteiden mukaan. Muita tietoja käyttäjistä ei tarvita testin käynnistämiseksi. Avoimessa testissä vähimmäismäärä testaajia on 1000 henkilöä, mutta enimmäismäärää ei halutessa tarvitse asettaa. Sovelluksesta voi olla samaan aikaan käynnissä suljettu ja avoin testi. (78; 79)

Android käyttöjärjestelmä sallii iOS käyttöjärjestelmää paremmin pääsyn järjestelmän sisäisiin komponentteihin. Pääsy mahdollistaa monipuolisempien sovelluksien tekemisen. Tavallisten mobiilisovellusten lisäksi sisäisten komponenttien avulla voidaan luoda esimerkiksi niin sanottuja laukaisijasovelluksia (*launcher*) ja muiden sovellusten päällä kelluvia sovelluksia. Laukaisijasovelluksilla voidaan muuttaa koko käyttöjärjestelmän ulkonäköä ja käyttäytymistä. (80; 81; 82)

4.2 Muut osat kehitystä

Sovelluksen kehitykseen liittyy muutakin kuin vairsinaisen sovelluksen kehitys. Osa sovelluksen toiminnallisuudesta saattaa vaatia palvelimen pystyttämistä ja käyttämistä. Käyttäjien tiedot halutaan mahdollisesti pitää tallessa tietokannassa, yhteys sovellusten välillä saattaa olla helpointa laittaa kulkemaan palvelimen kautta ja voi myös olla, että mobiilisovellus on vain yksi lisäkeino käyttää verkossa toimivaa itsenäistä palvelua.

Yksinkertaisempiinkin sovelluksiin saatetaan haluta sovelluksesta erillään oleva ja mahdollisesti keskitetty tietokanta käyttäjien tiedoille ja sisällölle. Palvelinta voidaan käyttää myös ilmoitusten (*push notification*) lähettämiseen käyttäjän laitteeseen. Ilmoitukset ovat palvelimelta käyttäjän laitteeseen lähtevä viesti. Se voi sisältää esimerkiksi tekstiä, kuvia ja interaktioita (83; 84). Ilmoituksilla voidaan lähettää käyttäjälle sovellukseen liittyvää informaatiota, esimerkiksi ongelmista, päivityksistä tai uudesta sisällöstä. Niillä voidaan myös koittaa aktivoida käyttäjiä, jotka eivät ole käyttäneet sovellusta lähiaikoina.

4.3 Mobiiliteknologiat

Mobiilisovelluksia voidaan kehittää usealla eri teknologialla, joista jokaisella on omat vahvuudet, heikkoudet ja erityispiirteet. Ne voidaan jakaa karkeasti kolmeen eri kategoriaan: natiivi, hybridi ja web. Eroja on muun muassa siinä kuinka hyvin teknologialla pääsee käsiksi laitteen komponentteihin ja voiko samaa koodia käyttää usealla eri alustalla. Sovelluskehittäjän on valittava teknologioista se, mikä sopii sovellukselle ja projektille parhaiten. Tässä luvussa käydään läpi eri mobiiliteknologiavaihtoehdot.

4.3.1 Natiivit teknologiat

Natiivilla teknologialla tarkoitetaan alustan oman ohjelmointikielen käyttämistä sovelluksen kehittämiseen. Usein alustavalmistaja tarjoaa kehitykseen myös oman ohjelmistoympäristön (*integrated development environment, IDE*). Natiivit teknologiat tarjoavat parhaiten pääsyn laitteen alustaan ja komponentteihin. Tämän ansiosta natiiveilla teknologioilla on mahdollista luoda paras käytettävyys, mobiili kokemus ja parhaat ominaisuudet. Niiden vahvuuksia ovat nopeat grafiikat, sulavat animaatiot ja monikosketus ominaisuudet, kuten kaksoisnapautus, nipistys ja levitys. Natiiveilla teknologioilla sovelluksesta saa myös tehtyä helpoiten järjestelmän omien ainutlaatuisten piirteiden ja muotoilujen mukaisen. Natiivien teknologioiden heikkouksia ovat hitaampi ja työläämpi kehitys. Jokaisen muutoksen jälkeen projekti on uudelleenkäännettävä ennen kuin sitä voidaan testata. Tämä hidastaa kehitystyötä erityisesti isommissa projekteissa, joissa kääntäminen saattaa viedä huomattavasti aikaa. Natiiveilla teknologioilla toteutetut sovellukset toimivat usein vain yhdellä alustalla. Kehitys on siten työlästä erityisesti silloin, kun kehitetään samaa sovellusta usealle eri alustalle. Sovelluksen lähdekoodia ei voida suoraan jakaa alustojen kesken. Natiiveja teknologioita käytettäessä ja kun sovellus halutaan julkaista monella alustalla kehittäjän tarvitsee mahdollisesti osata useita eri ohjelmointikieliä, käyttää kehityksessä eri ohjelmistoympäristöä ja osata eri rajapintojen (*application programming interface, API*) käyttöä tai jokaista alustaa varten, jolle sovellus julkaistaan tarvitaan eri kehittäjät. Jos halutaan kehittää vain yhdelle alustalle, niin natiivit teknologiat rajaavat käyttöalustoja, jolloin kehitys voidaan keskittää juuri näiden alustojen mukaiseksi. (80; 85; 86; 87; 88; 89)

Tunnetuimpia natiiveja teknologioita ovat esimerkiksi ohjelmointikielet Swift ja Objective-C, joita käytetään sovellusten kehittämiseen Applen tuotteille ja ohjelmointikieli Java, jota käytetään Android-pohjaisille laitteille kehittämiseen. Android käyttöjärjestelmälle suunnattu IDE on Android Studio ja iOS käyttöjärjestelmän vastaava on Xcode. (80; 86; 87; 90;)

4.3.2 Webteknologiat

Webteknologiat käyttävät kehitykseen webohjelmointiin tarkoitettuja kieliä, kuten HTML5, JavaScript ja CSS. Webteknologioilla tuotettua koodia ajetaan laitteen selainsovelluksella, kuten Googlen Chrome selaimella ja Applen Safari selaimella. Webteknologioiden vahvuus on koodin jakaminen alustojen välillä ja koodin toimiminen suurilta osin samalla lailla joka alustalla. Koodia voidaan jakaa myös suoraan verkkopalveluiden kanssa. Webteknologioiden heikkouksia ovat esimerkiksi vajaa pääsy laitteen komponentteihin, monikosketusominaisuuksien toteuttamisen vaikeus ja huonompi tehokkuus. Huono pääsy laitteen komponentteihin vaikeuttaa sellaisten sovellusten luomista, jotka käyttävät esimerkiksi kameraa, mikrofonia, kompassia, kiihdytysanturia, monikosketusominaisuuksia, ilmoituksia tai yhteydetöntä tilaa. (87; 91; 92; 93)

Facebook on yksi suurista yrityksistä, jotka käyttivät webteknologioita hyväkseen sovelluksessaan. Pääosin HTML5 teknologialla tehty sovellus auttoi heitä käyttämään samaa koodia usealle eri alustalle kehittäessä. Vuonna 2012 Facebook kuitenkin joutui tekemään kokonaan uuden sovelluksen natiiveilla teknologioilla, koska HTML5 teknologiaa hyödyntävä sovellus oli liian hidas. (88; 94)

4.3.3 Hybriditeknologiat

Hybriditeknologioissa käytetään yhdessä natiiveja teknologioita ja webteknologioita. Ne koostuvat yleensä ohuesta natiiveilla teknologioilla luodusta pohjasta, jonka päällä ajetaan webteknologoilla tuotettuja ominaisuuksia. Webteknologioiden hyödyntäminen onnistuu Webview luokan avulla. Webview luokka mahdollistaa Internetissä olevan sisällön näyttämisen sovelluksen sisällä. Luokka löytyy niin iOS kuin Android käyttöjärjestelmistä. Hybridin suurin hyöty on siinä, että samaa koodia voidaan käyttää eri alustoilla ja päästään myös käsiksi laitteen sisäisiin komponentteihin. Natiiveilla teknologioilla tehty pohja pitää tehdä joka käyttöjärjestelmälle erikseen, mutta sen päällä olevat webteknologioilla tuotetut ominaisuudet voidaan suoraan siirtää järjestelmästä toiseen. On hyvä kuitenkin huomata, että joka järjestelmässä on omat ainutlaatuiset piirteet ja muotoilut, joita kannattaa noudattaa. Tästä aihetta käsitellään tarkemmin luvussa 4.5.3. Muita hybriditeknologioiden hyötyjä on sovelluskoodin nopea kääntäminen, kehittäminen teknologioilla ei vaadi suuria määriä natiivien ohjelmointikielten osaamista ja helppo käyttö pilvipalveluiden kanssa. (87; 95) Hybriditeknologioiden huonoja puolia on yhdistelmä natiivien teknologioiden ja webteknologioiden huonoista puolista. Jo aiemmin mainitun natiivin pohjan uudelleen luomisen joka alustalle lisäksi hybridien teknologioiden käyttämä Webview luokka rajoittaa teknologioilla luotavia sovelluksia. Koodin uudelleen käyttö eri alustoilla ei välttämättä ole niin hyödyllistä, kuin voisi aluksi olettaa. Jos sovelluksen halutaan seuraavan alustan omia piirteitä, niin siirrettävän koodin muokkaaminen saattaa vaatia yhtä paljon vaivaa kuin oman natiiveilla teknologioilla luodun sovelluksen kehittäminen. (87; 91)

Hybriditeknologioita ovat myös teknologiat, jotka koodin kehittämisen jälkeen kääntävät koodin natiiveille kielille. Tällainen teknologia on esimerkiksi Facebookin kehittämä React Native. Se on React Javascriptkirjaston pohjalta tehty avoimen lähdekoodin Javascriptkirjasto natiivisti esitettävien mobiilisovellusten tekemiseen. React Native kirjastolla tuotettua koodia voidaan jakaa alustojen välillä. Niin kuin muillakin hybridi sovelluksilla, React Native kirjastolla on pääsy puhelimen ominaisuuksiin, kuten kameraan ja sijaintiin. React Native käyttää puhelimen omia natiiveja esitysrajapintoja alustasta riippuen Objective-C ohjelmointikielellä tai Java ohjelmointikielellä. Tästä syystä React Native kirjastolla kehitetty sovellus näyttää ja käyttäytyy kuin natiivi sovellus. (89; 96)

4.3.4 Visuaaliset työkalut

Kolmen teknologiakategorian lisäksi on hyvä käsitellä erikseen koodin tuottamiseen luodut visuaaliset työkalut. Ne ovat ohjelmia, jotka auttavat kehittäjää luomaan sovelluksia monelle alustalle visuaalisen käyttöliittymän kautta. Visuaaliset työkalut voivat käyttää mitä vain aiemmin mainituista kolmesta teknologiasta. Visuaaliset työkalut voivat tarjota kehittäjälle mahdollisuuden luoda sovellus ilman että kehittäjän tarvitsee osata ohjelmoida. Ne voivat myös tarjota mahdollisuuden toteuttaa sovelluksen jollain tunnetulla ohjelmointikielellä tai ohjelman ainutlaatuisella yksityiskielellä. Visuaalisten työkalujen haitta on, että kehittäjä menettää hallinnan lopputuloksen koodista. Jos lopputulokseen tehdään suoraan muutoksia, niin se ei ole enää synkronoitu alkuperäisen koodin kanssa. Lopputuloksen ylläpito ja hallinta voi olla haasteellista ja joudutaan helposti yhden toimittajan lukkoon (*vendor lock*). Yhden toimittajan lukko on tilanne, jossa organisaatio on riippuvainen yhdestä toimittajasta tai teknologiasta ja toiseen vastaavaan vaihtaminen ei ole mahdollista käytettävissä olevilla resursseilla. Lukosta seuraavat ongelmat voivat olla esimerkiksi mahdottomuus uusien ominaisuuksien kehittämiseen tai asiakastoiveisiin vastaamiseen.

4.4 Jakelu ja julkaisu

Sovellusten jakeluun on muutama erilainen keino. Sovellus voidaan esimerkiksi asentaa suoraan halutulle laitteelle, jakaa julkisesti Internetin yli tai se voidaan ladata sovelluskauppaan, josta sen voi löytää kaupan jokainen käyttäjä. Tässä luvussa käydään tarkemmin läpi sovellusten erilaisia jakamistapoja.

4.4.1 Sovelluskaupat

Sovelluskauppa on globaali, virtuaalinen kauppa, joka myy muun muassa sovelluksia, kirjoja, musiikkia ja elokuvia. Kaksi suurinta sovelluskauppaa ovat Applen App Store ja Googlen Play. Nämä ovat myös oman käyttöjärjestelmänsä virallisia kauppapaikkoja ja oletussovelluksia kyseisen käyttöjärjestelmän sisältävissä laitteissa. App Store on iOS

käyttöjärjestelmän sovelluskauppa ja Google Play on Android käyttöjärjestelmän vastaava. Kehittäjä voi luoda kehittäjätunnukset palveluihin. Näiden tunnusten avulla kehittäjä voi luoda sovelluksia ja julkaista ne sovelluskaupassa. Jos kehittäjän tuote myydään kaupassa, niin osa tuotoista menee sovelluskaupalle. (17; 75; 78; 97; 98; 99) Kaupoista tuotteet löytyvät sovelluksen nimeä, kuvausta, kategoriaa, arvosanaa ja hakusanoja hyväksi käyttäen. Käyttäjät voivat myös arvostella niitä ja jättää kommentteja kehittäjille ja muille käyttäjille. (17; 99)

4.4.1.1 App Store

App Store sovelluskaupassa julkaisuun ei tarvitse maksaa erillisiä maksuja. Kehittäjällä tulee kuitenkin olla voimassa olevat kehittäjätunnukset. Kaupassa myydystä tuotteista kehittäjä saa 70% hinnasta ja 85% jatkuvista tilausmaksuista. Apple hoitaa maailmanlaajuisesti maksujen käsittelyn. (74; 75) App Store sovelluskaupasta ladataan vähemmän sovelluksia kuin Google Play sovelluskaupasta, mutta käyttäjät kuluttavat niihin enemmän rahaa (3).

App Store sovelluskauppaan julkaiseminen on monivaiheinen prosessi. Sovelluksen valmistuttua ensimmäinen vaihe julkaisuun on sovelluksen projektin asetusten julkaisukuntoon asettaminen. Tämä tarkoittaa esimerkiksi sovelluksen tietojen täyttämistä, sovellukselle ikonin asettamista ja tuettujen laitetyyppien listausta. Täysi lista vaadituista tiedoista löytyy Applen kehittäjäsivuilta. Kaikki vaaditut asetukset löytyvät projektin yleisten asetusten välilehdeltä. Osaa näistä tiedoista ei voi muokata julkaisun jälkeen, joten niiden kanssa tulee olla huolellinen. (100; 101) Kun projektin tiedot ovat kunnossa on aika testata sovellusta. Sovellus voidaan testata laitteilla asentamalla sovellus niihin. Laite, jolle sovellus asennetaan, tulee olla rekisteröity kehittäjätilille. Rekisteröimiseen tarvitsee laitteen ainutlaatuisen laitetunnuksen. Laitetunnuksen saa iOS laitteille iTunesin kautta. Asentaminen voidaan tehdä suoraan Applen Xcode kehitysympäristön kautta laitteelle. Toinen vaihtoehto on luoda sovelluksesta iOS App tiedosto. Tämän tiedoston avulla laitteen käyttäjän ei tarvitse päästä fyysisesti käsiksi laitteeseen, jossa on sovelluksen koodi ja Xcode asennettuna. iOS App tiedosto luodaan arkistoinnin kautta. Testiversion jakamiseen testaajille löytyy myös monia muita keinoja. Nämä kaikki ovat listattu Applen kehittäjäsivuilla. (102)

Seuraava askel on ladata sovellus iTunes Connect palveluun. iTunes Connect palvelun avulla hallinnoidaan julkaistavaa sisältöä, sopimuksia, hinnoittelua ja niin edelleen (103). Palveluun ladataan arkistoitu versio sovelluksesta. iTunes Connect vaatii myös tietoja sovelluksesta. (104) Viimeiset askeleet ennen sovelluksen siirtymistä App Storeen ovat sovelluksen lähetettävän version valitseminen, iTunes Connect palvelun viimeisiin kysymyksiin vastaaminen ja sovelluksen lähettäminen arvioitavaksi. Arvioinnin suorittavat ihmiset ja se tulee takaisin joko hyväksyttynä tai hylättynä. Jos laite hylätään arvioinnissa, se tulee korjata ja lähettää uudelleen arvioitavaksi. Arvioinnin kesto voi vaihdella. Applen tietojen mukaan 50% arvioinneista on suoritettu vuorokauden sisällä ja yli 90% 48 tunnin sisällä. (80; 105; 106)

4.4.1.2 Google Play

Google Play sovelluskaupan kautta kehittäjä saa 70% sovellusten ja niiden sisältämien tuotteiden myyntituloista. Jäljelle jäävä 30% menee Googlen mukaan levityskumppaneille ja toimintamaksuihin. (107) Verrattuna App Store sovelluskauppaan, kuluttajat käyttävät vähemmän rahaa Google Play sovelluskaupan kautta, mutta lataavat huomattavasti enemmän sovelluksia (3).

Sovelluksen julkaiseminen Google Play sovelluskauppaan on monivaiheinen prosessi. Kun sovellus on valmis, siitä luodaan kehitysohjelmalla APK-tiedosto (*Android application package, APK*). APK-tiedostot ovat Android käyttöjärjestelmässä käytettäviä sovelluksen asennustiedostoja. APK-tiedoston lataaminen Google Play kauppaan tapahtuu Play Console sivuston kautta. Vuonna 2015 Google Play otti myös käyttöön hyväksyttämisprosessin sovelluksille. Prosessi on pyritty pitämään nopeana ja tavoitteena on prosessin läpivienti tunneissa päivien tai viikkojen sijaan. (108; 109; 110) Sovelluksen lataamisen jälkeen sovellukselle valitaan nimi, täytetään alustavat tiedot ja ladataan graafiset resurssit, kuten näyttökuvat ja esittelyvideo. Kaikista näistä voidaan luoda lokalisoidut versiot myös. Jos sovelluksen kehittäjä ei toimita omia käännöksiään, käyttäjä voi kääntää sovelluksen tiedot omalle kielelleen automattisella kääntäjällä. Valmistajan on hyvä tietää, että kääntäjä saattaa tehdä virheitä käännöksessä. Nämä virheet voivat haitata sovelluksen suosiota ja mahdolliset käyttäjät voivat olla lataamatta sovellusta näiden virheiden takia. Ensimmäisen askeleen jälkeen sovellukselle täytetään lisätietoja, kuten kategoria, yhteystiedot ja tietosuojamenettelyt. Lopuksi tulee vielä valita hinnoittelu ja jakoasetukset, sekä arvioida sovelluksen sisältö. Arviointi suoritetaan kyselyyn vastaamalla. (108; 109; 111)

4.4.1.3 Muut sovelluskaupat

Sovelluskaupat eivät rajoitu vain näihin kahteen tunnetuimpaan kauppaan. Android käyttöjärjestelmän sovellukselle vaihtoehtoisia sovelluskauppoja ovat esimerkiksi Amazon ja Slide Me. (112; 113) iOS käyttöjärjestelmän sovellukselle löytyy erityisesti sovelluskauppoja, jotka ovat suunnattu laitteille, joille on suoritettu Jailbreak-operaatio. Jailbreak-operaatio iOS käyttöjärjestelmälle ja Android laitteille suunnattu Root-operaatio ovat mobiililaitteille suoritettavia operaatioiota, joilla voidaan muokata käyttöjärjestelmää (1). Niitä voidaan käyttää esimerkiksi käyttöjärjestelmän rajoitusten kiertämiseen (1). Jailbreak laitteille kohdistuvia sovelluskauppoja ovat esimerkiksi AppCake ja Cydia. (114; 115) Cydia lasketaan paketinhallintajärjestelmäksi, mutta on samantapainen sovelluskauppojen kanssa. Mikään ei estä julkaisemasta sovellusta moneen eri sovelluskauppaan samaan aikaan (116).

4.4.2 Itsenäinen jakelu

Sovellukset voidaan myös jakaa itsenäisesti ilman sovelluskauppoja. Sovelluskaupat helpottavat sovelluksen saamista suuren yleisön ulottuville, mutta itsenäisessä jakelussa on

omat hyvät puolensa. Itsenäinen jakelu on oikea vaihtoehto esimerkiksi silloin, kun sovellusta ei haluta levittää sovelluskaupassa tai sovellus halutaan julkaista vain tietylle pienelle määrätylle joukolle. Sovellus voi olla esimerkiksi ainoastaan yrityksen sisäiseen käyttöön. Siinä tapauksessa sen jakaminen sovelluskaupassa ei olisi käytännöllistä. (17)

Apple tarjoaa yritysohjelmaa, jonka avulla sovelluksia voidaan julkaista ilman App Storen käyttöä. Se maksaa 299 Yhdysvaltain dollaria vuodessa (117). Yritysohjelmassa sovelluksen julkaisu alkaa samalla tavalla kuin App Storeen julkaisu. Se ei kuitenkaan käytä ollenkaan iTunes Connect palvelua. Sovelluksesta tehdään arkisto, jonka avulla luodaan iOS App tyyppinen tiedosto. Tämän tiedoston avulla käyttäjät voivat asentaa sovelluksen omaan laitteeseensa. (118) On tärkeää käyttää kehittäjätunnuksen sertifikaattia, kun sovellus julkaistaan App Storen ulkopuolella. Jollain laitteilla ja käyttäjillä voi olla päällä turvatoimia, jotka estävät sovellusten asennusksen, joista sertifikaatti puuttuu. On myös hyvä muistaa, että kun julkaistaan App Storen ulkopuolelle, niin osa Applen palveluista eivät ole käytössä. (119)

Android käyttöjärjestelmän sovelluksille itsenäinen julkaisu onnistuu jakamalla APK-tiedoston. Tiedoston saajalla tulee olla esto tuntemattomista lähteistä ladatuille tiedostoille poissa päältä. APK-tiedoston voi julkaista omilla verkkosivuillaan tai lähettää kohteelle, vaikka suoraan sähköpostilla. Yksi tämän tavan heikkouksista on hallinnan puute. Tiedoston saaja voi itse jakaa sovelluksen yksinkertaisesti välittämällä APK-tiedoston eteenpäin. Tämä voi tietysti olla myös haluttua toimintaa. (116) Veikkaus OY valitsi itsenäisen jakamisen vaihtoehdon, kun heidän sovelluksensa poistettiin Googlen toimesta Google Play sovelluskaupasta. Sovellus on ladattavissa heidän verkkosivuillaan. Veikkaus OY kertoo sivuillaan poiston syyksi, että sovellus mahdollistaa rahapelauksen. (120)

4.5 Mobiilikehityksen yleiset haasteet

Mobiililaitteita on monenlaisia. Puhelimet, älykellot ja muut vastaavat ovat usein pieniä ja kevyitä, kun taas tabletit ja vastaavat ovat isompia ja raskaampia. Mobiililaitteet kulkevat käyttäjän mukana ja niitä käytetään monissa erilaisissa ympäristöissä. Mobiililaitteiden erityispiirteet luovat mobiilikehitykseen sille luonteenomaisia haasteita. Tässä luvussa käsitellään ongelmia, jotka tulevat yleisesti vastaan, kun kehitetään sovelluksia mobiililaitteille.

4.5.1 Mobiililaitteiden pienet resurssit

Nykyajan suosituimmissa mobiililaitteissa kuten puhelimissa ja tableteissa on valtava määrä tehoa pieneen kokoonsa nähden, mutta laitteiden suoritusresurssit ovat kuitenkin rajalliset. Mobiililaitteiden pieni koko asettaa rajoitteita niihin asennettavien komponenttien kanssa ja kaiken kaikkiaan niiden kapasiteetit ovat usein pienempiä kuin muilla tietokoneilla. Langattomat siirtonopeudet vaihtelevat alustasta, liittymästä ja käyttäjän sijainnista riippuen. Samat ohjelmaratkaisut eivät välttämättä toimi mobiililaitteissa niin

kuin muissa tietokoneissa. Tässä luvussa käsitellään, miten resurssien vähyyteen voidaan reagoida ja miten niitä voidaan mahdollisesti kasvattaa fyysistä laitetta muuttamatta.

4.5.1.1 Laitteen pieni koko ja rajalliset komponentit

Verrattuna suurempiin laitteisiin, mobiililaitteissa on paljon pienemmät resurssit. Näytön koko on pienempi, fyysinen tila rajoittaa suuren näppäimistön sisällyttämistä, laitteen fyysiset napit ovat pieniä tai niitä ei ole ollenkaan ja niin edelleen. Nämä rajoitteet on otettava huomioon jo suunnitteluvaiheessa, kun mietitään mobiilisovelluksen toimintaa ja käytettävyyttä. Mobiililaitteissa saattaa olla tuki ominaisuuksille kuten eleet, kosketus, sormenjäljen tunnistaminen, kamera, sijainnin seuraaminen, kiihtyvyyden ja liikkeen tunnistus ja muille vastaaville. Kyseisiä ominaisuuksia hyödyntämällä voidaan luoda hyviä käyttöliittymiä ja paikata aiemmin mainittuja rajoitteita. Tämä on tärkeää erityisesti tietoturvan kanssa. Muualla käytetyt tietoturvaratkaisut eivät välttämättä toimi mobiililaitteissa. Pahimmassa tapauksessa käyttäjä kiertää ne kokonaan käytettävyyden parantamiseksi. Esimerkiksi sisäänkirjautuminen luo turvallisuutta, mutta tekee yhden lisäaskeleen tehtävän suorittamiselle ja siten häiritsee käyttäjää. Jos sisäänkirjautumista pitää toistaa useita kertoja tai sen suorittaminen on mobiililaitteella haasteellista, niin sovelluksen käyttökokemus kärsii.

4.5.1.2 Datan säilytys

Datan säilytykseen mobiililaitteissa liittyy joitakin erityispiirteitä. Yleensä mobiililaitteiden pienen fyysisen koon takia, niihin ei saada sisällytettyä yhtä paljoa muistia kuin esimerkiksi pöytätietokoneisiin. Haasteeseen on erilaisia ratkaisuja. Sama data voi olla monessa eri muodossa. Mobiililaitteen pienen muistin ja vaihtelevien siirtonopeuksien takia datan muoto on hyvä pitää sellaisena, joka vie vähän tilaa ja on helppo siirtää huonoillakin siirtonopeuksilla. Palvelimella data saatetaan haluta pitää eri muodossa, esimerkiksi siksi, että sitä on nopea käyttää. Tällöin data voidaan muokata. Datan muokkaaminen on tärkeää keskittää palvelimelle. Dataa siirrettäessä, mobiililaitteen tulisi lähettää data palvelimelle mobiililaitteelle sopivimmassa muodossa. Palvelin vastaanottaa tämän datan, muokkaa sen itselleen sopivaksi ja käyttää sitä haluamallaan tavalla. Jos palvelimelta tarvitsee lähettää dataa mobiililaitteille, se tulee muokata ensin mobiililaitteille ja pienemmille siirtonopeuksille sopivaan muotoon palvelimella, jotta sen siirtäminen ja käyttöönotto mobiililaitteen päässä olisi nopeampaa.

4.5.2 Korkeat laatuvaatimukset

Mobiililaitteet ovat yleistyneet ympäri maailmaa. Vuosien varrella sovellukset ovat parantuneet ja käyttäjille on muodostunut kuva siitä, mikä on hyvä sovellus ja mikä ei. Kuluttajille suunnatut pelit ja interaktiiviset sovellukset ovat luoneet korkeat käyttökokemusvaatimukset (1). Ohjelmistokehittäjälle voi tulla yllätyksenä käyttäjien suuret vaatimukset käytettävyydessä, tehokkuudessa ja yleisessä toimivuudessa. Vaatimukset ovat tärkeä täyttää, jos sovellus aiotaan julkaista sovelluskaupassa. Sovelluskaupat sisältävät

käyttäjien arviointeja. Näihin arviointeihin vaikuttaa käyttäjien kokemukset sovelluksen käytöstä. Osa käyttäjistä saattaa jättää sovelluksen kokonaan lataamatta, jos arvosanat ovat huonoja.

4.5.3 Monta eri alustaa

Tietyissä tapauksissa saattaa olla mahdollista määritellä, että sovelluksen tulee toimia vain yhdellä tietyllä alustalla, mutta on todennäköisempää, että sovelluksen tulee toimia usealla eri alustalla. Vaatimus usean alustan tukemiseen voi tulla esimerkiksi asiakkaalta tai käyttäjältä. Mobiililaitteissa erilaisten alustojen määrä on huomattavan suuri. Jo pelkästään älypuhelimissa on monta eri käyttöjärjestelmää, käyttöjärjestelmien versioita, valmistajaa, näyttökokoja ja puhelimien malleja. Sama pätee muihinkin mobiililaitteisiin. Näitä yhdistelemällä saadaan varsin suuri määrä mahdollisia kohdealustoja. Vaikka alustoilla olisi samankaltaiset fyysiset kapasiteetit, niin laiteen käyttöjärjestelmän sisäiset erot sekä kehitykseen käytetty ohjelmointikieli ja ohjelmointimalli voivat olla hyvinkin erilaiset. Käyttöjärjestelmän sisällä eroja on muun muassa sovelluksen ikonissa, palkeissa, navigaatiossa ja typografiassa. Erilaisten alustojen määrä on suuri erityisesti Android käyttöjärjestelmässä. Android mahdollistaa muutokset järjestelmän sisäisiin komponentteihin iOS käyttöjärjestelmää vapaammin, jonka ansiosta monet valmistajat luovat muutoksia tai kokonaan oman version käyttöjärjestelmästä. Kehityksessä voidaan koittaa panostaa saman sovelluksen tai ohjelmakoodin toimivuuteen usealla alustalla, mutta se tuo lisähaasteita. (1; 80; 121)

Usealle alustalle kehitettäessä on varauduttava moneen eri osaamisvaatimukseen. Alustojen ominaisuuksien ja piirteiden tunteminen, mobiilisovellusten ohjelmointikielet ja käyttöjärjestelmien suunnitteluohjeiden tunteminen ovat esimerkkejä tarvittavasta osaamisesta. Erityisesti, jos halutaan kehittää sovellus monelle alustalle käyttäen natiiveja teknologioita, tarvitaan monenlaista osaamista. (1; 80; 121) Vanhojen versioiden ja niiden tukemat ominaisuudet on hyvä osata, jos käyttäjistä moni omistaa vielä vanhan version käyttöjärjestelmästä. Uuden ominaisuuden lisääminen saattaa tarkoittaa sovelluksen käytön estämistä usealta käyttäjältä. Usealle alustalle kehitettäessä ja testattaessa myös resurssivaatimukset kasvavat. Mobiilialustoilla on omat kääntö- ja kehitysympäristöt. Esimerkiksi Applen iPhone älypuhelimille kehittämiseen tarvitaan macOS käyttöjärjestelmä. Sovellusten testaaminen tulisi suorittaa jokaiselle kohdelaitteelle erikseen. Usean erilaisen testauslaitteen hankkiminen voi tulla kalliiksi. Erilaisten laitteiden lisäksi testauksessa eroina on myös laitteen ulkopuoliset tekijät, kuten sijainti, liittymä ja verkko. (1; 80)

Sovellukselle tulee luoda yhtenäinen käyttöliittymä alustasta riippumatta, mutta samalla ottaa huomioon alustan ainutlaatuiset piirteet ja muotoilut. Kun sovellus on yhtenevä alustoista riippumatta, on käyttäjän helppo vaihtaa laitetta ja silti jatkaa sovelluksen käyttöä. Tästä on myös hyötyä esimerkiksi tapauksessa, jossa sovelluksen käyttäjä haluaa

neuvoa toisella alustalla sovellusta käyttävää ystäväänsä. Alustan piirteiden huomioiminen taas auttaa käyttäjää, joka on jo alustan piirteet oppinut ja sisäistänyt, navigoimaan ja käyttämään sovellusta. Käyttäjät haluavat, että sovellus näyttää, tuntuu ja toimii kuin mihin hän on tottunut. Sovellusta ei voida täten suoraan siirtää toiselle alustalle. Esimerkiksi navigointi iOS ja Android käyttöjärjestelmissä on erilainen jo pelkästään sen takia, että Android käyttöjärjestelmän sisältävissä älypuhelimissa on erillinen nappi, jolla pääsee navigaatiopolussa taaksepäin. Applen iOS käyttöjärjestelmälle kehitettäviin sovelluksiin tulee luoda oma nappi käyttöliittymään takaisinpäin navigointiin. (1; 80; 121) Alustoilla on myös yhteisiä ominaisuuksia. Niitä käyttäen voidaan luoda sovellus, joka on helpommin siirrettävissä alustojen välillä. Ääriesimerkki yhteisten ominaisuuksien hyödyntämisestä alustariippumattoman sovelluksen luomiseen on mahdollisimman yhtenäisen toteutuksen taktiikka. Taktiikka perustuu siihen, että sovelluksessa käytetään vain yksinkertaisimpia ominaisuuksia, jotka löytyvät joka alustalta. Taktiikkaa noudattamalla vältetään eri alustojen monimutkaisuuksia ja sama toteutus toimii joka alustalla, mutta sitä ei suositella. Vain yksinkertaisimpia ominaisuuksia käyttämällä menetetään käyttöliittymien ainutlaatuiset ominaisuudet ja sovelluksesta tulee liian yksinkertainen. (1)

4.5.4 Huonot yhteydet

Mobiilisuuteen liittyy usein myös langattomuus. Langattomien yhteyksien laatu riippuu useasta eri tekijästä. Laitteen sisältämä teknologia on niistä ensimmäinen. Erilaisten alustojen suuren määrän takia myös mahdollisten yhteyskomponenttien määrä on suuri. Eri verkkotekniikoiden ja nopeuksien tukeminen vaihtelee. Toinen tekijä on laitteen liittymä. Kahdessa samanlaisessa laitteessa saattaa olla erilainen yhteys siihen liitetyn liittymän takia. Liittymä voi hallita yhteyden määrää tai nopeutta. Pahimmassa tapauksessa liittymä ei anna yhteyttä ollenkaan. Kolmas tekijä on laitteen sijainti verkkoon nähden. Mobiililaitteita käytetään mitä moninaisimmissa paikoissa. Eri alueiden kuuluvuus vaihtelee. Kaupungeissa saattaa olla hyvä kuuluvuus, kun taas sen ulkopuolella ei ole välttämättä verkkoa lainkaan. Infrastruktuuri, kuten tunnelit ja rakennusten seinät ja katto, haittaavat kuuluvuutta, vaikka oltaisiin muuten hyvällä kuuluvuusalueella. (1)

Yhteyttä ottavien laitteiden määrä saattaa myös ylittää verkon kapasiteetin, jolloin laitteeseen ei saada ollenkaan yhteyttä. Näin voi tapahtua juhlapäivinä, jos väki kerääntyy suurella joukolla juhlimaan yhdessä, tai massatapahtumissa, kuten konsertit ja festivaalit. Yksi tämänkaltaisista tapahtumista oli Chicagossa järjestetty Pokémon Go mobiilipelin ensimmäinen suuri tosielämän tapahtuma. Tapahtuman noin 20 000 osallistujaa kuormittivat mobiiliverkot ja pelin palvelimet tehden tapahtumassa pelaamisen mahdottomaksi. (122; 123; 124; 125; 126) Huonoihin yhteyksiin voidaan varautua tallentamalla tarvittava tieto laitteeseen ja päivittämällä sitä yhteyden löytyessä. Tieto voidaan myös yrittää luoda laitteesta itsestään. (1)

4.5.5 Ratkaisuja palvelimilla

Osa mobiilisovellusten yleisistä haasteista saadaan ratkaistua mobiililaitteen ulkopuolisilla resursseilla, kuten palvelimilla. Palvelimella tarkoitetaan yleensä fyysistä laitetta, joka tarjoaa tietoteknisiä resursseja ja palveluita yhteyden kautta, mutta sillä voidaan myös tarkoittaa pilvipalvelua. Pilvipalvelut ovat kokoelma palvelimien varannoksi koottuja resursseja, jotka jaetaan usean käyttäjän kesken heidän tarpeidensa mukaan. Palvelimen resursseja voidaan kasvattaa periaatteessa loputtomiin lisäämällä komponentteja tai laitteita. (1)

Palvelimet voivat esimerkiksi toimia lisäresursseina mobiililaitteelle, nopeuttaa kehitystyötä tai auttaa laitehallinnassa. Niissä voidaan säilyttää paljon dataa käyttämättä mobiililaitteen omaa fyysistä muistia. Laitteella voidaan säilyttää lista ja esimerkiksi esikatselun mahdollistavat pienet osat datasta. Kun käyttäjä haluaa käyttää tätä dataa, se haetaan palvelimelta. Käytön jälkeen data tallennetaan taas laitteen ulkopuolelle ja laitteen muisti vapautuu. Vapautuneen muistin lisäksi, lataamalla data palvelimelle, se on turvassa myös laitteen kadotessa tai rikkoutuessa. Kun laitteen sisäinen muisti voidaan jättää pieneksi, vapautuu tilaa myös laitteen fyysisestä alueesta. Vapautunut tila voidaan käyttää hyväksi laitteen muiden ominaisuuksien parantamiseen. (1)

Palvelimet voivat olla yksityisiä, julkisia tai niiden risteymiä. Yksityistä vaihtoehtoa käytetään vain yksittäisen yrityksen tai ryhmän toimesta. Se tarjoaa julkisia enemmän hallintamahdollisuuksia ja ovat hyvä valinta, jos resursseihin liittyy tärkeitä yrityksen tai loppukäyttäjien tietoja. Yrityksen arkaluontoinen ja valtioon tai terveydenhuoltoon liittyvä tieto ei ole välttämättä asianmukaista tallentaa julkiselle palvelimelle. Julkisista palveluista ei aina tiedä minne data tallennetaan ja kuka niihin pääsee käsiksi, joten niitä tulee käyttää vain jos ne sopivat projektin tietoturvallisuudesta määritettyihin vaatimuksiin. Julkiset palvelimet ovat tarkoitettu suurelle yleisölle ja niiden käyttöönotto on usein yksityisiä vastaavia halvempaa ja helpompaa. Yritys voi mukauttaa halutunlaisen palvelun tarpeidensa täyttämiseksi yksityisen ja julkisen palvelimen risteymällä, niin sanotulla hybridipalvelimella. Ennen palvelimen käyttöönottoa on hyvä käydä läpi kaikki sen vaikutukset. Palvelin, josta maksetaan käytön mukaan, saattaa pitkässä käytössä tulla kalliimmaksi kuin yrityksen oma sisäinen ratkaisu. (1)

Mobiili ja pilvipalvelut ovat teknologioita, joista usein puhutaan yhdessä toisiaan vahvistavina teknologioina. Pilvipalvelut voidaan ottaa käyttöön ja poistaa käytöstä nopeasti. Pilvipalvelut ovat hyvä vaihtoehto, jos omaa palvelinta tai back-end infrastruktuuria ei haluta tai pystytä tekemään. Pilvipalvelut saattavat näyttää houkuttelevilta erityisesti pienille yrityksille, joilla ei ole taitoa tai varaa luoda ja ylläpitää monimutkaista tietojenkäsittely-ympäristöä. Ne voivat olla myös korvaamattomia tilanteissa, joissa resurssien tarve on vaihtelevaa tai väliaikaista. Näissä tilanteissa pilvipalveluja voidaan hyödyntää käsittelemään ylimääräiset resurssitarpeet. Pilvipalveluja tarjoavat yritykset tekevät voit-

toa tarjoamalla resursseja. Pilvipalveluihin on luotu standardeja, mutta silti monet palvelut ovat pilvikohtaisia. Pilvikohtaisuus tekee toiseen pilveen siirtymisestä vaikeaa. Palveluita käyttäessä on myös pysyttävä poissa niin kutsutusta yhden toimittajan lukosta. (1)

Mobiilikehityksen yhtenäinen piirre on lyhyet kehitysaikavaatimukset. Vaatimukset nopealle kehitykselle tekevät mistä tahansa mobiiliprojektista haasteellisen. Työryhmällä ei ole aina varaa käyttää viikkoja back-end järjestelmien asentamiseen, testaamiseen ja virheiden korjaamiseen. Valmiina käyttöön olevat resurssit sovelluksen käyttöön voivat nopeuttaa kehitysaikaa huomattavasti. Toimivan varastointi-, tietoturva- tai verkkoratkaisun uudelleen keksimisen sijaan voi olla järkevää käyttää palvelua, jossa on kaikki tarvittava jo valmiina. MBaaS pilvipalvelut ovat juuri tällaiseen tilanteeseen luotu vaihtoehto. MBaaS on lyhenne mobiilista back-end palvelusta (*mobile back end as a service, MBaaS*). MBaaS pilvipalvelulla saadaan maksua vastaan projektille valmis ja toimiva back-end. Se voi huomattavasti vähentää mobiiliprojektin hintaa ja monimutkaisuutta, sekä nopeuttaa valmistumista. (1) Pitkällä tähtäimellä se saattaa kuitenkin tulla kalliiksi palvelun käyttömääristä, hinnoittelusta ja hinnoittelun muutoksista riippuen.

Pienellä tai aloittavalla yrityksellä ei usein ole suurta alkupääomaa, jolla luoda hienostunutta IT infrastruktuuria. Isot yritykset usein kokeilevat mobiiliratkaisujen tekemistä ja projektit saattavat jäädä lyhyiksi. Molemmissa tapauksissa nopean ja vain pienen alkusijoituksen vaativan pilvipalvelun käyttöön ottaminen on järkevää. Pilvipalvelun avulla voi aloittaa nopeasti, maksaa käytön mukaan ja lisätä resursseja tarvittaessa. Kun mobiiliprojekti todistaa tuottavuutensa, voidaan pilvipalvelu tarvittaessa vaihtaa perinteiseen infrastruktuuriin. Ympäristö itsessään voi myös vaatia pilvipalveluiden käyttöä. Uusien markkina-alueiden infrastruktuuri ei ole välttämättä sovelias mobiiliprojektin tarpeisiin. Etäältä tapahtuva mobiili-infrastruktuurin käyttö voi olla äärimmäisen tärkeää kasvavilla markkinoilla, joista puuttuvat tarvittavat laitteet, verkot ja ohjelmisto infrastruktuurit. Tällaisissa tapauksissa kokonainen mobiili-infrastruktuuri pilvipalveluna voi olla korvaamaton. (1)

Pilvipalveluita voidaan hyödyntää myös kehitys- ja testausympäristöjen hallinnassa. Eri alustojen kehittämiseen ja kääntämiseen tarvittavat ympäristöt voidaan ottaa käyttöön pilvipalvelusta, jolloin kehitykseen ei tarvitse hankkia omia fyysisiä laitteita. Mobiililaitteiden testaamiseen tarvittavan laitemäärän hallinnointi, jakaminen eri kehitystiimien kesken ja päivitys uusien mallien myötä voidaan tehdä fyysisten laitteiden sijaan virtuaalisesti. Pilvipalveluun perustuva mobiilisovellusten testausympäristön kautta kehitystiimi saa verkon yli käyttöönsä suureen määrään erilaisia mobiililaitteita, jotka ovat yhteydessä verkkoon eri puolilla maailmaa. Tällä tavalla kehitystiimillä on käytössä monta eri laitetta niin manuaaliseen kuin automatisoituunkin testaukseen. Periaatteessa kehitystiimi vuokraa testaukseen tarvitsemansa laitteet testauksen ajaksi. Mobiililaitteet voidaan alustaa useanlaiseen sijaintiin ympäri maailmaa, joten testauksessa saadaan huomioitua kyseisen sijainnin verkko. Testauksen jälkeen laitteet palautetaan pilvipalvelun varantoon. Pilvi-

palvelun avulla vältetään fyysisten laitteiden ylläpito ja hallinnointi ja saadaan testausympäristö, joka on käytettävissä tarvittaessa. Pilvipalvelun laitteita voidaan lisätä ja vaihtaa milloin vain. Tarvittaessa testit voidaan suorittaa samalla laitteella virheiden toistamiseksi tai niiden korjauksen varmistamiseksi. (1)

4.6 Tietoturva

Mobiililaitteiden erityisominaisuudet tekevät myös sille suunnatuista tietoturvaratkaisuista omanlaisensa. Tietoturva on otettava huomioon jo kehitysvaiheessa, jotta mahdolliset haavoittuvuudet voidaan estää. Tässä luvussa käsitellään mobiililaitteisiin liittyviä tietoturvapiirteitä, sekä tietoturvariskejä ja niiden mahdollisia ratkaisuvaihtoehtoja.

4.6.1 Tietoturvauhat

Turvallisen sovelluksen kehittämiseksi on tunnettava suurimmat mobiiliin liittyvät uhat ja hyökkäystekniikat.

4.6.1.1 Haitalliset ohjelmat

Mobiilihaittaohjelma (*mobile malware*) on ohjelma tai skripti, joka on suunniteltu häiritsemään mobiililaitteita, keräämään arkaluontoista informaatiota tai mahdollistamaan luvaton pääsy laitteelle. Mobiilissa esiintyviä haitallisia ohjelmia ovat muun muassa vakoiluohjelmat, virukset, madot ja troijalaiset.

Vakoiluohjelma (*spyware*) on ohjelma, joka asennetaan kohteen laitteelle tämän tietämättä. Se kerää salaa tietoa tai tarkkailee kohteen käyttäytymistä. Kerättyä tietoa voi olla esimerkiksi tunnus ja salasana yhdistelmät, pankkitiedot tai kohteen verkkokäyttäytyminen. Kaupallinen vakoiluohjelma nimeltä FlexiSpy tarjoaa kotisivuillaan sovellukselle seuraavia ominaisuuksia:

- Lue pikaviestintäsovellusten viestit.
- Kuuntele puheluita reaaliajassa.
- Lue SMS- ja sähköpostiviestit.
- Kuuntele puhelimen ympäristöä.
- Katso puhelimen sijainti.
- Vakoile mitä vain puhelinta.
- Saa käyttöösi tunnukset ja salasanat.
- Yhteensä yli 150 ominaisuutta. (127)

Lista antaa kuvan mahdollisista tiedonkeruukeinoista, joita vakoiluohjelmasta löytyy. Haitalliseen käyttöön kehitetty ohjelma saattaa sisältää vielä enemmän ominaisuuksia ja kapasiteettia kuin kaupalliseen tarkoitukseen kehitetty (1).

Virukset ja madot voivat kopioida itsensä ja siirtyä mobiililaitteesta toiseen esimerkiksi verkkoyhteyden yli (1). Haittaohjelmat toimivat kahdessa vaiheessa: leviäminen ja toiminta. Leviämisvaiheessa virus kiinnittää itsensä toiseen ajettavaan tiedostoon. Virus leviää, kun tiedostoa siirretään tai jaetaan uusiin ympäristöihin. Toisin kuin virukset, madot voivat toimia itsenäisesti. Esimerkiksi Nimda niminen mato käyttää sen sisäänrakennettua sähköpostiprotokollaa itsensä levittämiseen. Toimintavaiheessa haittaohjelma aktivoituu ja toimii sen kehittäjä haluamalla tavalla. Toiminta voi olla mitä vain näytölle tekstinmuotoisen viestin kirjoittamisesta ja mainosten näyttämisestä aina kovalevyn ylikirjoittamiseen asti. (128)

Troijalainen tai troijan-hevonen tarkoittaa ohjelmaa, joka vaikuttaa ulkoapäin vaarattomalta, mutta on oikeasti kykenevä haitalliseen toimintaan. Troijalaisen saaminen mobiililaitteeseen tapahtuu yleensä väärennetyn tai muokatun mobiilisovelluksen avulla. Käyttäjä luulee väärennettyä tai muokattua sovellusta aidoksi ja lataa sen mobiililaitteeseen. Lataamisen jälkeen sovellus saattaa silti toimia kuin aito, mutta pitää sisällään mahdollisuuden haitalliseen toimintaan. (1)

4.6.1.2 Hyökkäykset

Hyökkäykset eroavat haitallisista ohjelmaista siten, että ne eivät välttämättä tarvitse erillistä ohjelmaa käyttäjän laitteelle aiheuttaakseen haittaa. Mobiililaitteita vastaan tehtyjä hyökkäyksiä ovat esimerkiksi sosiaalinen tiedustelu, SQL-injektio, istunnon kaappaus, palvelunesto hyökkäys ja QR-koodi huijaus.

Sosiaalinen tiedustelu (*social engineering*) käyttää hyväkseen kohteen luottamusta johonkin. Tiedustelussa pyritään saamaan kohde huijattua asentamaan mobiilihaittaohjelma tai antamaan arkaluontoista tietoa. Tietoa kohteen sosiaalisesta kontekstista hyödynnetään lisäämään totuudentuntua huijaukseen. Mobiililaitteisiin liittyvään sosiaaliseen tiedusteluun yhtenä keinona voidaan käyttää monen tekijän todennusta (*multi-factor authentication*). Monen tekijän todennus tarkoittaa nimensä mukaan monen eri tekijän käyttämistä yhdessä käyttäjän todentamiseen. Se on nykyisin yleinen turvallisuuskäytäntö. Yksi esimerkki monen tekijän todennuksesta on puhelimen kautta tapahtuva todennus. Käyttäjän rekisteröityessä palveluun, hänelle lähetetään puhelimeen koodi, joka tulee syöttää palveluun. Näin saadaan suurempi varmuus, että käyttäjä on kuka hän väittää olevansa. Hyökkäävä taho saattaa käyttää hyväkseen sitä, että käyttäjä on tottunut tämän kaltaiseen todennukseen. Kohde voidaan huijata asentamaan saastunut sovellus mobiililaitteeseen saadakseen palveluun syötettävän koodin. Toinen sosiaalisen tiedustelun esimerkki on tietojen kalastelu (*phishing*). Tietojen kalastelu on prosessi, jossa hyökkääjä esittää luotettavaa lähdettä ja saa käyttäjän luovuttamaan arkaluontoista tietoa, vierailemaan haitallisella sivulla tai ajamaan haitallista koodia. Mobiilimaailmassa tietojen kalastelua voidaan tehdä muun muassa äänen tai tekstimuotoisten viestien avulla. (1)

SQL-injektiossa (*SQL injection*) hyökkääjä syöttää skriptimuotoista dataa mobiilisovelluksen lomakkeeseen. Jos skripti ajetaan palvelussa, niin hyökkääjä voi saada yhteyden

tietokantaan ja siten poistaa, kopioida tai muuten käyttää väärin tietokannan sisältöä. Yhteyden muodostamisen jälkeen hyökkääjä voi aloittaa palvelunestohyökkäyksen (*denial-of-service, DoS*) tai muuttaa palvelimen esimerkiksi lähettämään roskapostia. SQL-injektion voi estää käyttämällä nykyaikaisia tietokantoja tai tarkistamalla syötteet ennen käyttöä. Palvelunestohyökkäyksen tarkoituksena on tehdä palveluun pääsy mahdottomaksi. Se voidaan kohdistaa myös mobiililaitteisiin. Yksi vaihtoehto hyökkäykselle on lähettää tuhansia tekstiviestejä laitteeseen. Toinen vaihtoehto on etsiä haavoittuvuuksia käyttöjärjestelmästä ja väärinkäyttää niitä. (1) Näin tapahtui iPhone puhelimien kanssa pariinkin otteeseen. Kohteelle lähetettiin viesti, jossa oli tekstiä, jota iOS käyttöjärjestelmä ei osannut käsitellä oikein. Viestin vastaanottaminen aiheutti ongelmia laitteessa, kuten laitteen jäätymisen tai uudelleenkäynnistymisen. (129; 130)

Istunnon kaappaus (*session hijacking*) on hyökkäys, jossa hyökkääjä hankkii ja käyttää hyväkseen kohteen istuntoa. Istunnolla tarkoitetaan käyttäjän tilaa palvelussa. Istunto voi pitää sisällään esimerkiksi tiedon siitä onko käyttäjä kirjautunut sisään vai ei, ja mitä tavaroita käyttäjällä on palvelun ostoskorissa. Istunnon kaappaamalla hyökkääjä pääsee käsiksi tähän tilaan ja suorittaa toimia käyttäjän sijaan tai aloittaa väliintulohyökkäyksen (*man in the middle, MitM*). Väliintulohyökkäyksessä hyökkääjä sijoittaa itsensä käyttäjän ja palvelun väliin. Hyökkääjä voi lukea ja vaikuttaa käyttäjän ja palvelun välillä siirrettävään dataan. Tämän kaltainen hyökkäys tapahtuu todennäköisesti avointa verkkoa käytettäessä. Istunnon kaappauksen välttämiseksi tulee käyttää suojattua yhteyttä avoimessa verkossa asioidessa. (1)

Haittaa hakevat tahot saattavat yrittää saada käyttäjiä vierailemaan haitallisilla verkkosivuilla. Yhtenä keinona tähän toimivat linkit, joiden määränpäätä ei voi tietää etukäteen. Mobiililaitteille suunniteltuja QR-koodit eivät ole ihmiselle luettavassa muodossa ja ne avataan mobiililaitteen kameran avulla. Käyttäjä voidaan huijata avaamaan QR-koodin sisältämä linkki, joka vie hänet haitalliselle sivulle. Tätä kutsutaan QR-koodi huijaukseksi (*QR code spoofing*). (1)

4.6.1.3 Tietovuoto

Tietovuoto tarkoittaa yksityisen datan päätymistä väärille tahoille. Mobiililaitteet ja niiden ympäristö sisältävät erityisiä ominaisuuksia, jotka voivat lisätä tietovuodon riskiä:

- Viestinnän kaappaus. Mobiililaitteita saatetaan käyttää julkisissa verkoissa, joiden kautta haitalliset tahot voivat koittaa kaapata viestinnän.
- Synkronointi tietokoneen tai palvelun kanssa. Automaattinen synkronointi voi siirtää myös yksityistä dataa suojaamattomaan laitteeseen tai palveluun.
- Liitteet ja katseluohjelmat. Tiedostot, joiden avaamiseen tarvitaan erillinen ohjelma asettavat tiedoston vaaraan. Erillinen katseluohjelma voi olla kolmannen osapuolen tuottama eikä sen rehellisyydestä ole takeita. Toisinaan katseluohjelma luo kopion tiedostosta mahdollisesti epäturvalliseen osaan laitetta.
- Leikkaus ja liittäminen. Informaatio saatetaan siirtää suojatusta muodosta epäsuojattuun leikkaamalla ja liittämällä.

- Ulkoinen muisti. Ulkoiselle muistille tallennettu data voi liikkua ulkoisen muistin mukana väärään paikkaan. (1)

Vuodetun tiedon skaala on suuri. Se voi olla esimerkiksi arkaluontoista yksityistietoa, luottamuksellisia asiakastietoja, yrityssalaisuuksia, työntekijöiden tietoja tai tulevan tuotteen lähdekoodia. Yritysten tietovuotoihin liittyy kaksi suurta informaatioryhmää: immateriaalioikeudet ja määräysten mukainen informaatio. (1) Immateriaalioikeudet ovat muun muassa tekijänoikeuksia ja patentteja. Ne ovat monelle yritykselle sen tärkein voimavara. Määräysten mukainen informaatio on erityisesti terveydenhuoltoon perustuvalle yritykselle suuressa roolissa. Potilastietoihin liittyy monia säännöksiä ja niiden rikkomisesta tai noudattamatta jättämisestä saattaa olla huomattavia seurauksia (131). Säännösten noudattaminen voi olla haastavaa mobiililaitteiden lisätessä monimutkaisuutta ja nostaessa rikkomuksen tapahtumisen riskiä (1).

Tietovuodolla on monenlaisia seurauksia. Seuraukset voivat olla rahallisia menetyksiä sakkojen muodossa, syytteitä, kilpailukyvyn tai edun menettäminen, regulaattorisia toimenpiteitä, huonoa julkisuutta ja asiakkaiden menettämistä. (1) Ponemon Instituutin ja IBM:n 2016 tekemän tutkimuksen mukaan keskimääräiset tietovuodosta aiheutuvat kustannukset ovat 4 miljoonaa Yhdysvaltain dollaria. Hinta yhdelle vuodetulle dokumentille nousi 2015 vuoden 154 Yhdysvaltain dollarista 158 dollariin. Tutkimuksen mukaan suurin rahallinen menetys tulee liikevaihdon menetyksestä. Yrityksen tulee palauttaa asiakkaiden luotto pitkäaikaisten menetysten estämiseksi. Suurimmat tietovuotojen aiheuttajat tutkimuksen mukaan ovat rikolliset tai haitalliset hyökkäykset (48%). Järjestyksessä seuraavaksi suurimmat syyt olivat järjestelmien toimintahäiriöt (27%) ja inhimilliset erehdykset (25%). Terveydenhuollon alalla tietovuodon aiheuttamat tappiot ovat keskivertoa suuremmat. Tämä johtuu sakoista ja keskivertoa suuremmasta liikevaihdon ja asiakkuuksien menetyksestä. (132) Ponemon Instituutin ja IBM:n 2016 tekemästä tutkimuksesta selviää myös ennaltaehkäisyn suuri rooli haittojen minimoimisessa, sekä salauksen ja päätepisteiden turvallisuuden tärkeys. Suurin kustannuksia vähentävä tekijä on kuitenkin erillisen kriisiryhmän olemassaolo. Tutkimuksen mukaan tietovuodon kustannuksia kasvattavia tekijöitä erityisesti mobiililaitteisiin liittyen ovat laaja pilvipalveluiden käyttöön siirtyminen ja laitteiden hukkuminen. (132)

4.6.2 Mobiililaitteiden erityiset tietoturvapiirteet

Mobiililaitteiden tietoturvariskit ovat monin tavoin samanlaisia kuin muilla tietotekniikkaan liittyvillä osa-alueilla, mutta ainutlaatuisen luonteensa takia on olemassa joitakin mobiililaitteille ominaisia tietoturvaan liittyviä piirteitä. Ennen älypuhelimia mobiililaitteisiin kohdistuva haitallinen aktiviteetti oli rajallista. Laitteet ja niiden ohjelmistot valmistivat yksittäiset valmistajat ja mobiililaitteiden sisältämien ohjelmien toiminnallisuus oli rajattua. Mobiililaitteiden erojen ja rajatun toiminnallisuuden takia ne olivat alustana epäsuotuisa hyökkäyksille. Hyökkäykset eivät toimineet usealla alustalla suoraan ilman muutoksia. Nykyisin mobiililaitteet ovat toiminnallisuuksiltaan monipuolisempia, niihin

käsiksi pääseminen on helpompaa ja useampi osa laitteista käyttää samaa käyttöjärjestelmää. Nämä ominaisuudet johtavat niihin vaikuttavien haitallisten toimintojen määrän kasvuun. Mobiililaitteet omaavat usein monia eri keinoja olla vuorovaikutuksessa ympäröivän maailman kanssa. Erilaisten verkkoyhteyksien ja muistinkäsittelykeinojen, kuten Wi-Fin, Bluetoothin, puhelinverkon, muistikorttien ja pilvisäilöjen takia tarvitaan entistä enemmän suojautumiskeinoja luvattoman pääsyn ja datan menetyksen estämiseksi. Laitteisiin pääsee käsiksi myös sovellusten avulla. Kolmannen osapuolen sovelluksia ladataan mobiililaitteiseen aktiivisesti sovelluskaupoista tai muista lähteistä. Vaikka sovellukset itsessään eivät olisi haittaohjelmia, ne saattavat sisältää tietoturva-aukkoja, joita haitalliset tahot voivat hyödyntää. Pelkkä varovainen mobiililaitteen käyttö ei aina riitä takaamaan turvallisuutta, sillä laite voi saastua myös kanssakäymisestä saastuneen tietokoneen kanssa. Monet niistä uhista, jotka vaikuttavat jo tietokoneisiin, vaikuttavat tai tulevat todennäköisesti vaikuttamaan mobiililaitteisiin myös. Jo olemassa olevien riskien lisäksi uudet teknologiat, kuten esimerkiksi mobiilimaksaminen ja NFC-protokolla (*near field communication, NFC*), tuovat mukanaan vielä lisää tietoturvan riskitekijöitä. Tämä ei tietenkään tarkoita, etteikö uutta teknologiaa voisi ottaa käyttöön. Mobiililaitteiden tietoturvan on vain kehityttävä käsittelemään myös nämä uudet uhat. (1; 2; 133)

Datan suuri määrä ja keskittyminen tekevät mobiililaitteista oivan kohteen tietovarkauksille (1; 133; 134). Käyttäjä mahdollisesti haluaa hyödyntää mobiililaitteen siirrettävyyttä ja kätevyyttä esimerkiksi pankkitoimintaan, sosiaaliseen verkostoitumiseen, sähköpostitteluun ja kalenterin ja yhteystietojen hallinnointiin. Mobiililaitteiden ominaisuudet mahdollistavat myös sellaisen tiedon saamisen, jota ei normaalista tietokoneesta saisi. Tietokoneella ei ole välttämättä samalla tavalla pääsyä esimerkiksi käyttäjän sijaintiin tai tekstiviesteihin. (133) Mobiililaitteet saattavat sisältää suuret määrät niin henkilökohtaista kuin yrityksenkin tietoja ja resursseja. Mobiililaitteiden taipumus olla sosiaalisen vuorovaikutuksen välineenä mahdollistaa helpon informaation jakamisen ja siirtämisen yksilöiden välillä. Tämä voi altistaa myös arkaluontoisen informaation päätymisen vääriin käsiin. Jos laitteen käyttötarkoituksissa yhdistyy työ ja vapaa-aika, saattaa kaikkiin tarkoituksiin toimivan tietoturvamallin toteuttaminen olla haasteellista. Myös mobiililaitteiden laaja määrä ja erot laitteiden välillä, sekä mobiilisovelluksille ominaiset korkeat käyttökokemusvaatimukset voivat tehdä vaikeaksi yhtenevän tietoturvamallin luomisen. (1)

Muita mobiililaitteille ominaisia tietoturvaan vaikuttavia piirteitä ovat pieni koko, mahdollisuus liikkua käyttäjän mukana ja Jailbreak- tai Root-operaatiot. Mobiililaitteet nimensä mukaisesti liikkuvat käyttäjän mukana. Siirrettävyys ja laitteiden usein pieni koko ja keveys altistavat ne hukkumisriskille ja varkaudelle. Mahdollisuuden käyttää laitetta liikkeessä ja ennalta määräämättömissä paikoissa vuoksi laitetta saatetaan käyttää myös julkisissa verkoissa, jotka voivat olla tuntemattomia ja suojaamattomia. Pieni näyttö vaikeuttaa laitteen käyttämistä ja käyttäjälle voi olla vaikeata huomata pienet erot, jotka erottavat esimerkiksi aidon Internetsivun haitallisesta kopiosta. (1) Jailbreak- tai Root-operaatio antaa käyttäjälle oikeudet muokata käyttöjärjestelmää, mutta luo

myös riskin, että haittaohjelmat hyödyntävät näitä oikeuksia. Tärkein tietoturvatekijä on kuitenkin käyttäjä itse. Käyttäjän toiminta vaikuttaa vahvasti ja suoraan tietoturvaan.

4.6.3 Suojautuminen mobiiliuhkia vastaan

Mobiiliuhkia vastaan voidaan suojautua monella eri tasolla. Sovellusten suunnittelu kannattaa tehdä alusta alkaen tietoturva mielessä pitäen (1). Ottamalla tietoturvan huomioon sovellusten kehitysvaiheessa kooditasolla voidaan välttää monia mobiiliuhkia mahdollistavia tietoturvavirheitä. Sovellusten lisäksi uhilta voidaan suojautua laite- ja yhteystasolla. Käyttäjän toiminta vaikuttaa myös vahvasti suojautumiseen.

On hyvä pitää mielessä, että liian monimutkainen tai laitteen käyttöä estävä tietoturvapolitiikka haittaa käyttäjää ja pahimmassa tapauksessa ajaa käyttäjän etsimään mahdollisuuksia tietoturvan toteuttavien kokonaisuuksien kiertämiseen. Käyttäjä on hyvä eristää tietoturvan toteuttavista osioista. Mitä enemmän tapahtuu taustalla ilman, että käyttäjän tarvitsee siihen reagoida, sen parempi. Tämä vähentää käyttäjien virheistä johtuvia ongelmia. Käyttäjälle on kuitenkin hyvä kertoa, mitä taustalla tehdään luottamuksen säilyttämiseksi. (1; 2) Kun käyttäjän tietää mitä taustalla tehdään, hän voi myös omilla toimillaan seurata ja vahvistaa näitä taustaprosesseja.

4.6.3.1 Sovelluksen kehitysvaiheen tieturvatekijät

Sovellustason tietoturvan varmistaminen alkaa jo sovelluksen kehitysvaiheessa. Laitteen tai käyttöjärjestelmän kehityspaketti (*software development kit, SDK*) itsessään saattaa jo tarjota valmiita tietoturvan toteuttavia toimintoja, joita voidaan käyttää rajapintojen avulla. Kehitysvaiheessa pitää varmistaa, että sovellukseen ei tule synnynnäisiä tietoturvavirheitä. On yleensä halvempaa korjata tietoturvaan liittyvät ongelmat sovelluksen kehitysvaiheessa kuin sen valmistumisen jälkeen. Jos verkkosovelluksissa huomataan tietoturvaongelma, niin sen päivittäminen onnistuu suoraan palvelimelta. Jos mobiilisovelluksesta löydetään tietoturvavirhe, tekijä korjaa sen ja jakaa päivitetyn version sovelluskauppaan, käyttäjälle tai muuhun jakoväylään. Mobiilikäyttöliittymät eivät kuitenkaan pakota käyttäjää asentamaan sovellusten uusinta versiota. Käyttäjät ovat siis vapaita valitsemaan haluavatko he ladata ja asentaa uusimman päivityksen vai eivät. Tietoturvapäivitysten asentamista ei voi täten jättää käyttäjän varaan vaan päivityksen lataaminen tulee keinolla tai toisella pakottaa. Mobiilisovelluksen on hyvä pystyä varmistamaan, että käytössä on uusin version myös asennuksen jälkeen. (1) Sovelluksen voidaan esimerkiksi asettaa käytön estävä vipu, jota voidaan hallita sovelluksen ulkopuolelta. Sovellus tarkastaa vivun käynnistyksessä. Jos vipu on aktivoitu ja sovelluksen versio ei ole sama kuin uusin jaossa oleva versio, niin sovellus estää käytön ja antaa päivitysohjeet.

Kehitysvaiheessa voidaan käyttää erilaisia tekniikoita tietoturvan parantamiseksi. Näistä yksi on sovelluksen skannaus. Sillä etsitään sovelluksesta haavoittuvuuksia. Sovelluksen skannaus tunnistaa yleisiä haavoittuvuuksia, kuten SQL-injektion, selaimen käskytyksen

(*cross-site scripting*) ja selaimen pyynnönhuijauksen (c*ross-site request forgery*). Selaimen käskytyksessä hyökkääjä muuttaa verkkopalvelulle luotettavasta lähteestä tullutta koodia (135) ja selaimen pyyntöhuijauksessa hyökkääjä muokkaa käyttäjän palveluun lähettämää dataa (136). Sovelluksen skannaus koostuu yleensä valkolaatikkotestauksesta (*white box testing*) ja mustalaatikkotestauksesta (*black box testing*). (1) Valkolaatikkotestaus tunnetaan myös nimellä lasilaatikkotestaus. Se on testaustyyli, jossa tarkastellaan syötettä ja tulosta niin, että testaaja tietää järjestelmän sisäisen toiminnan ja rakenteen. Valkolaatikkotestauksen avulla löydetään heikkouksia koodista. Mustalaatikkotestaus on testaustyyli, jossa testaaja suorittaa testit pelkän syötteen ja tulosteen avulla ilman, että hänellä tarkkaa tietoa sovelluksen sisäisestä toiminnallisuudesta. Mustalaatikkotestaus on suunniteltu etsimään heikkouksia valmiista tai lähes valmiista sovelluksista. (135) Testaus suoritetaan aikajaksoittain sovelluksen tietoturvan tilan selvittämiseen (1).

4.6.3.2 Virustorjuntaohjelmat ja palomuuri

Mobiililaitteiden virustorjuntaohjelmalla voidaan etsiä haittaohjelmia käymällä läpi koodia laite- ja sovellustasolla, sekä muistikorteilta. Applen iOS käyttöjärjestelmälle on kuitenkin mahdotonta toteuttaa tämän kaltainen selausohjelma käyttöjärjestelmän sovellusten välisen eristyspolitiikan takia. (1) App Store sovelluskaupasta löytyy iOS käyttöjärjestelmälle tehtyjä virustorjuntaohjelmia, mutta ne eivät tarkastele laitteen sisäisiä toimintoja vaan kertovat käyttäjälle esimerkiksi haitallisista sivustoista ja tarjoavat ominaisuuden puhelimen sijainnin selvittämiseen tai sen sisältämien tietojen tyhjentämiseen (137; 138). Android-laitteelle selausohjelman voi toteuttaa, mutta ei ole selvää tarjoaako se saman tason turvan kuin pöytäkoneen virusturvaohjelma. Mobiililaitteiden palomuurin avulla voidaan tarkkailla sisään ja ulos menevää tietoliikennettä. Palomuuri voi rajata tietoliikennettä, jos se epäilee haitallista toimintaa laitteessa. Haitoilta voidaan suojautua myös haitallisten tahojen suodatuksella. Käyttäjiä voidaan esimerkiksi estää pääsemästä haitallisille sivustoille tai voidaan suodattaa pois tietyistä puhelinnumeroista tulevat puhelut ja tekstiviestit. (1) Ainoastaan tunnettujen uhkien etsiminen ei välttämättä riitä. Tietoturvatoteutuksesta saadaan parempi, kun se tunnettujen uhkien lisäksi tutkii laitteen käyttäytymistä ja etsii epäilyttävää toimintaa. Android käyttöjärjestelmässä toteutus voidaan suoraan sisällyttää käyttöjärjestelmään itseensä sovelluksen sijaan. (2; 139)

4.6.3.3 Käyttäjän tunnistus ja pääsyn hallinta

Käyttäjän tunnistus kuvaa kuinka varmistetaan, että käyttäjä on kuka hän väittää olevansa. Pääsynhallinta määrittää mitä käyttäjä saa palvelussa tehdä. Tunnistuksen ja pääsynhallinnan perimmäinen tarkoitus on saada tarpeeksi tietoa käyttäjästä, jotta heille voidaan antaa oikeat käyttöoikeudet. Mobiililaitteiden ainutlaatuisten ominaisuuksien takia niissä ei välttämättä toimi kaikki vanhat tunnistusmetodit, mutta ne tuovat monta uutta vaihtoehtoa. (1) Mobiililaitteiden käyttäjät eivät halua kirjoittaa pitkiä tunnuksia ja salasanoja. Tunnuksien syöttämistä vaikeuttaa laitteen pieni koko ja se, että erikoismerkkien tai numeroiden käyttäminen saattaa vaatia ylimääräisiä painalluksia. (1; 2) Käytettävyys kärsii erityisesti siinä tapauksessa, kun salasanoja joutuu syöttämään useita kertoja. Tässä

tapauksessa käyttäjä saattaa lähteä kiertämään ongelmaa ja valita helpommin syötettävän salasanan parantaakseen käytettävyyttä tai kopioida tunnukset niiden kirjoittamisen sijaan. Molemmat tavat laskevat laitteen tietoturvallisuutta. Mobiililaitteilla käytettävyyden ja turvallisuuden välillä tasapainottelu on jatkuvaa. Mahdollisuuksien mukaan mobiililaitteilla kannattaa käyttää vaihtoehtoisia tunnistautumismenetelmiä, koska perinteinen tunnistautuminen tunnuksella ja salasanalla ei ole yhtä vaivatonta mobiililaitteilla kuin pöytäkoneilla.

Kosketusnäyttöä hyödyntäen tunnistautuminen voi olla esimerkiksi näytöllä tietyn kuvion paineleminen, sormella kuvion piirtäminen, allekirjoituksen tekeminen, tietyn nopeuden ja voiman käyttö kuvion jäljentämisessä tai eleillä kuvion tekeminen. Kuvan hyödyntämiseen tunnistautumisessa voisi olla tiettyjen kohtien koskettaminen kuvassa oikeassa sarjassa, halutunlaisen kuvion piirtäminen tai oikeiden kuvien valinta isommasta ryhmästä. (1) Kuva 2 on esimerkki kuvion piirtämisestä. Keltainen viiva on käyttäjän piirtämä kuvio taustalla olevan kuvan päälle.

Kuva 2. Kuvioon perustuva käyttäjän tunnistus.

Kuvioon perustuvan tunnistuksen ongelmia on syötteen tarkkuuden määrittäminen. Pitää ottaa huomioon eri henkilöiden tavat tehdä syöte. Toinen tärkeä asia on kuvassa 3 esitetty tilanne, jossa kuvion piirtämisestä on jäänyt näyttöön jälkiä. Haitallinen taho saattaa keksiä kuvion, jos se tehdään useita kertoja samaan kohtaan. Tähän voidaan vaikuttaa siirtämällä kuvaa eri tunnistuskertojen välillä. (1)

Kuva 3. Näyttöön piirtämisestä jääneet jäljet.

Mobiililaitteilla voidaan hyödyntää monista laitteista löytyviä ominaisuuksia biometrisen kirjautumisen luomiseksi. Kameralla tunnistamiseen voidaan kuvata silmän retina, 3-D kasvot, silmien räpäytyssarja, käden muoto ja sormenjälki. Sormenjäljen lukemiseen voidaan käyttää myös sormenjälkilukijaa. Biometrisessä tunnistautumisessakin on ongelmana mittauksen tarkkuus. Toimiiko äänentunnistus meluisassa ympäristössä? Toimiiko kameralla tunnistautuminen vähäisessä valossa? Tarkkuutta voidaan lisätä erityislaitteistolla, mutta ylimääräinen laite haittaa käytettävyyttä ja saattaa olla riesaksi käyttäjälle. Mobiililaiden mahdollistamat tunnistusmenetelmät eivät rajoitu edellämainittuihin. Jos se on tarkoituksen mukaista, niin myös muita laitteen ominaisuuksia nykysiä tai tulevaisuudessa tulevia, kuten käyttäjän äänentunnistusta ja kiihtyvyysanturilla laitteen liikkeen mittaamista, voidaan käyttää tunnistautumiseen. (1)

Käyttäjän tunnistuksessa ja pääsynhallinnassa voidaan myös käyttää hyödyksi mobiililaitteiden mahdollista tietoa kontekstista. Esimerkiksi sijaintia tai kellon aikaa voidaan käyttää määrittämään käyttäjän oikeuksia. (1; 2) Toimistolla ollessaan tai työaikana käyttäjällä voidaan antaa pääsy arkaluontoisempaan materiaaliin kuin mitä hänellä olisi illalla kauppareissulla. Mobiililaitteiden käyttö osana monen tekijän todennusta on yleistynyt. Monen tekijän todennuksessa käytetään useaa eri todennusta käyttäjän tunnistukseen. Tunnuksen ja salasanan lisäksi käyttäjä saa esimerkiksi mobiililaitteeseen kertakäyttöisen numerokoodin, joka hänen tulee syöttää palveluun. Käytettäessä älypuhelinta mobiililaitteena säästetään käyttäjä erillisen mobiililaitteen mukana kuljettamisen vaivalta. Tämän kaltainen monen tekijän varmennuksen toimivuus on riippuvainen verkkoyhteydestä. Yhteydetöntä sisäänkirjautumista tarvitaan, jos sisäänkirjautumisella suojatulla järjestel-

mällä ei ole pääsyä verkkoon. Ilman verkkoa järjestelmä ei pääse käyttämään sisäänkirjautumiseen käytettävää infrastruktuuria. Tällöin käyttäjän todentamiseen tarvitaan vaihtoehtoisia keinoja. Salattua muistia voidaan käyttää hyväksi tämän toteuttamiseen. (1)

Menetelmästä riippumatta käyttäjän tunnistuksessa kannattaa pyrkiä käyttämään kertakirjautumista. Kertakirjautuminen tarkoittaa sitä, että käyttäjä pystyy käyttämään kaikkia palveluja yhdellä sisäänkirjautumisella. (1; 2) Jos mobiilisovellusta tehdään jo käytössä olevalle palvelulle, pitää huomioida, kuinka mobiililaitteet sopivat nykyiseen tunnistusjärjestelmään. (1)

4.6.3.4 Tiedon suojaus

Mobiililaitteiden käytön yleistyessä informaation suojausta on mietittävä uudelleen. Tietojen suojaaminen ulkopuolisilta vaatii paljon työtä. On tärkeää myös suojata tieto valumasta ulos sisäpuolelta. Pelkkä teknologinen varustautuminen ei riitä, vaan myös käyttäjä on otettava huomioon.

Tiedot voidaan suojata salaamalla ne. Kaikki arkaluontoinen laitteeseen tallennettu data pitäisi olla mahdollista salata. Salaaminen suojaa tietoja haittaohjelmilta ja vääriin käsiin päätymiseltä. Salaus on prosessi, jossa tiedosto muokataan käyttökelvottomaksi algoritmia hyväksikäyttäen. Tiedosto voidaan muokata takaisin luettavaan muotoon avaimen avulla. Käyttäjän näkökulmasta tämä tulisi tehdä taustalla esimerkiksi käyttäjän kirjautuessa sisään ja ulos. Salaukseen löytyy monia eri tapoja. Osa tavoista on mahdollistettu suoraan laitevalmistajan puolesta. Laitteiston valmistajien välillä voi olla kuitenkin eroja, jotka tulee ottaa huomioon monia eri laitteita käytettäessä. Mobiililaitteita käytettäessä tieto on suojattava ainakin kolmessa eri paikassa: palvelimilla ja tietokannoissa, mobiililaitteessa ja kun informaatio liikkuu näiden välillä. Palvelimilla ja tietokannoissa olevan tiedon suojaaminen voidaan tehdä perinteisillä menetelmillä. Tiedon lähetys saadaan suojattua ja salattua varmistamalla, että mobiililaitteessa ja palvelimella tai yhteyden toisella puolella on asianmukaiset ohjelmat. Salaus ei ole kokonaisvaltainen, jos liikkuvaa dataa ei salata. Salaamaton liikkuva tieto voidaan yrittää kaapata haitallisten tahojen toimesta. Itse laitteessa säilytettävän arkaluontoisen materiaalin määrää kannattaa rajoittaa mahdollisimman paljon mobiililaitteiden liikkuvan luonteen takia. Hukkuneen laitteen löytämistä voidaan helpottaa laitteen ominaisuuksilla. Laitteen GPS voi kertoa laitteen sijainnin, laitteen kaiuttimien kautta voidaan soittaa jokin äänimerkki, jonka etsijä voi kuulla, salamaa ja värinää voidaan käyttää esimerkiksi tilanteissa, jossa omistaja ei voi kuulla ääntä. Jos laitetta ei löydetä tai saada takaisin, niin se voidaan lukita tai tyhjentää etänä. Tällä tavalla estetään laitteen sisältämän tiedon päätyminen väärille tahoille. Tyhjennyksessä voidaan valita, tyhjennetäänkö koko laite, tietty osio laitteesta vai vain tietyn sovelluksen tiedot. (1)

Muita ratkaisuja tiedon suojaamiseen on sen eristäminen (*containerization*), kääriminen (*wrapping*) ja mobiilivirtualisointi (*virtualization*). Eristäminen on toimenpide, jolla yksi

tai useampi sovellus voidaan eristää suojattuun ympäristöön. Eristämällä sovellus ympäristöön voidaan se suojata hyökkäyksiltä ja tietovuodolta. Eristäminen mahdollistaa myös sovelluksien keskitetyn hallinnan. Eristäminen tapahtuu sovellustasoa ylemmällä työtilatasolla. Mobiilisovelluksen käärimisessä sovellus päällystetään tietoturvan toteuttavalla kääreellä. Kääriminen voidaan toteuttaa ilman aikaa vievää ja vaivalloista sovelluksen uudelleenkääntämistä tai päivittämistä. Kääriminen tarjoaa keinon hallinnoida sovelluksia laitetason sijaan sovellustasolla. Käärimisen avulla voidaan hallita sovelluksen käyttäjien oikeuksia, vahvistaa tietoturvaa, suojata tietovuodolta, tarkkailla sovelluksen käyttöä, tallentaa käyttöhistoriaa, toteuttaa korjaavia toimia sovellustasolla, kuten tyhjentää laitetta, estää käyttöä ja poistaa käyttäjiä käyttöryhmistä. Mobiilisovelluksen käärimisen vahvuus on, että sitä voidaan käyttää jo olemassa oleviin sovelluksiin. Kolmannen osapuolen sovellusten kääriminen saattaa kuitenkin olla haastavaa. Kääriminen vaatii sovelluskaupan kiertämisen ja sovelluksen koodin ja päivitysten saamisen suoraan kehittäjältä. Mobiilia virtualisointia voidaan käyttää luomaan eristetty osio mobiililaitteeseen. Siitä on tullut lupaava teknologia datan ja sovellusten hallinnan ongelmien ratkaisuun mobiililaitteiden tehokkaan tietojenkäsittelyn ansiosta. Apple ei salli virtuaalikoneen asentamista laitteisiinsa, mutta Android käyttöjärjestelmissä se voi tarjota huomattavia tietoturvaa parantavia ominaisuuksia. (1)

4.6.3.5 Yhteyksien suojaus

Yhteyden suojaaminen on tärkeä linkki hyökkäysten torjumisessa. Mobiililaitteet käyttävät yhteyden muodostukseen useita eri väyliä. Esimerkiksi puhelinverkkoa, langattomiaverkkoja ja Bluetooth-teknologiaa. Mikä vaan näistä tavoista voi avata reitin haitallisille tahoille. Mobiiliverkon suojaamisella suojataan kommunikaatioväylä sovelluksen ja palvelun välillä. (1)

Tärkein mobiiliverkon suojausmekanismi on virtuaalinen mobiiliyksityisverkko (*mobile virtual private network, mVPN*). Virtuaalinen yksityisverkko (*virtual private network, VPN*) on tietoliikennetekniikassa menettely, jolla yhdistetään eri toimipaikoissa sijaitsevia lähiverkkoja ja päätelaitteita käyttäen siirtotienä julkisia verkkoja (140). Virtuaalinen mobiiliyksityisverkko on mobiiliversion tästä menettelystä. Se käyttää turvallisen yhteyden aikaansaamiseksi monia salaus- ja todennustekniikoita, joilla varmistetaan tietojen eheys, käyttäjän tunnistus, käyttöoikeuksien hallinta, luottamuksellisuus ja näin mahdollistetaan tietojen turvallinen siirto (140). Kehittyneempiä ominaisuuksia virtuaaliselle mobiiliyksityisverkolle ovat yhteyden laadun optimointi verkon toimintakyvyn mukaan ja lisäturvan tarjoaminen tunnistamalla, jos laite ei ole turvallinen tai suojaamaton ja rajoittamalla liikennettä. (1)

4.6.3.6 Laitteen ja sovellusten hallinnointi

Sovelluksen käyttöä voidaan rajoittaa sallimalla sen ajaminen vain tietyistä laitteista. Käytetty laite tunnistetaan esimerkiksi laitteen yksikäsitteisen identifikaation avulla. Laitteen identifikaatiota verrataan sallittujen laitteiden listaan. Tarkistaminen voidaan myös

tehdä pelkästään sovelluksen asennuksen yhteydessä. Palvelinta käytettäessä, voidaan sovelluksia ja laitteita rajoittaa sen kautta. Palvelimen rajoituksilla voidaan koittaa suojautua esimerkiksi muokatuilta sovelluksilta aitouden testaamisella. Muokattu sovellus on uusi versio alkuperäisestä sovelluksesta, johon on lisätty haitallista koodia. Palvelin ja sovellus voivat tunnistaa toisensa ja vahvistaa toistensa aitouden. Kun palvelin tunnistaa yhteyden tulevan tuntemattomasta sovelluksesta, se voi estää yhteyden. Sovellus voi myös tunnistaa onko se yhteydessä aitoon palvelimeen vai ei. Aitouden testaamisella voidaan suojautua myös MitM-hyökkäykseltä. (1)

Nykyiset kuluttajille suunnatut sovelluskaupat eivät välttämättä täytä yritystason vaatimuksia hallinnan, valvonnan tai tietoturvallisuuden suhteen. Ratkaisuna toimii yrityksen oma sisäinen sovelluskauppa. Se hallitsee yrityksen hyväksymiä ja sen omia sovelluksia. Omaa sovelluskauppaa käyttäen voidaan hallita mitä sovelluksia käyttäjät voivat ladata ja siten vähentää haitallisten sovelluksien lataamista. Myös yksittäisten käyttäjien sovellusten käyttöä pystytään oman sovelluskaupan avulla valvomaan. (1) Toimivan sisäisen sovelluskaupan tulisi sisältää seuraavat ominaisuudet:

- Tuki usealle laitetyypille ja käyttöjärjestelmälle. Esimerkiksi Android ja iOS käyttöjärjestelmät.
- Mahdollisuus tukea montaa erityyppistä sovellusta. Esimerkiksi natiiveja, hybridi ja websovelluksia. Myöskin yrityksen itse kehittämiä ja kolmannen osapuolen sovelluksia.
- Kaiken kattava identiteetti ja tunnistusjärjestelmä käytön valvomiseen.
- Pääsynhallinta sovelluksien lataamiseen ja käyttöön.
- Käyttäjille ilmoitusten lähettämismahdollisuus. Esimerkiksi huoltoon tai päivittämiseen liittyvissä tapauksissa.
- Sovellusten etäpäivittämisen mahdollisuus.
- Ohjesääntö sovellusten lataamiseen, käyttämiseen ja jakamiseen.
- Sovellusten lataamisen salliminen vain yrityksen sisäisestä sovelluskaupasta.
- Käyttäjien palautteen ja arvostelujen kerääminen.
- Käytön, lisenssien ja oikeuksien hallinnointi. (1)

Mobiililaitteiden keskitetyllä hallintaohjelmalla (*mobile device management, MDM*) suojataan, valvotaan ja hallinnoidaan mobiililaitteita. Ohjelma suorittaa toimenpiteitä, joilla varmistetaan, että laite on turvallinen. Hallinnan mahdollistaa sovellusten, tietojen ja asetusten etäjakaminen. Laite voidaan lukita tai tyhjentää etänä, jos se varastetaan tai se hukkuu. Hallinnalla voidaan varmistaa, että salasanat ovat yrityksen politiikan mukaisia ja päivitetty. Myös laitteen toiminnallisuutta voidaan valvoa ja tiettyjä toimintoja voidaan rajata. Esimerkiksi pilvitallennus halutaan mahdollisesti estää, jotta laitteessa oleva tieto ei sitä kautta leviä väärille tahoille. Lopuksi voidaan varmistaa, että yrityksen verkkoon kuuluvat laitteet ovat yrityksen tietoturvaohjeiden mukaisia. (1; 134) Seuraavat asiat on mahdollista toteuttaa MDM-ohjelmassa:

- Laitteeseen suoritetun Jailbreak/root-operaation havaitseminen.
- Laite- tai sovellustasolla toteutettu laitteen etälukitus ja -tyhjennys.

- Salauksen käytön varmistaminen.
- Yrityksen linjan mukaisen salasanan/PIN-koodin käytön takaaminen.
- Sijaintiin perustuvia tietoturva-asetuksia. Esimerkiksi yrityksen tiloissa laitteella on enemmän oikeuksia, kuin yrityksen tilojen ulkopuolella.
- Integraatio jo olemassa olevien järjestelmien kanssa.
- Laiteinventaario.
- Laitteiden asetusten konfigurointi etänä.
- Käyttöoikeuksien hallinta.
- Laitteen verkkovierailun tunnistaminen ja siihen reagointi.
- Kulutushallinnointi.
- Etäpäivitys järjestelmälle ja sovelluksille.
- Etäkäyttö.
- Vain sallittujen sovellusten asentamisen salliminen tai kiellettyjen sovellusten asennuksen estäminen.
- Mahdollisuus ilmoittaa käyttäjälle, jos laite ei ole määräysten mukainen ja ohjata käyttäjää tekemään tarvittavat muutokset.
- Aitouden testaus. (1)

Joukolle sovelluksia voidaan tehdä erillinen mobiilisovellusten hallinnointiohjelma (*mobile application management, MAM*). MAM-ohjelma keskittyy pelkästään sovelluksiin laitteen hallinnoinnin sijaan. Sillä voidaan esimerkiksi pyyhkiä yrityksen mobiilisovellukset ja data laitteesta, sekä estää niiden käyttö tulevaisuudessa, ilman että kosketaan laitteen muihin sovelluksiin tai dataan. (1; 134)

5. YHTEENVETO

Työssä tutkittiin, mitä tulee ottaa huomioon, kun lähdetään toteuttamaan mobiilisovelluksia terveydenhuollon tarpeisiin, miten mobiili toimii alustana terveydenhuollon sovelluksille ja miten terveydenhuollon lait ja säädökset vaikuttavat kehitykseen. Näiden lisäksi käytiin läpi kaksi suurinta mobiilikäyttöjärjestelmää ja kolme eri mobiiliteknologiaa, sekä sovellusten julkaisu, mobiilikehityksen yleiset haasteet ja mobiilisovellusten tietoturvaan liittyviä piirteitä.

Mobiili toimii alustana terveydenhuollon sovelluksille hyvin. Mobiililaitteiden ansiosta terveydenhuolto ei ole enään paikkaan sidottua. Mobiililaitteet ovat teknologisesti kehittyneitä, halpoja ja laajasti käytettyjä. Ne sisältävät sensoreita ja tekniikkaa, joita voidaan käyttää hyväksi terveydenhuollon sovelluksissa. Terveydenhuolto asettaa erityisiä vaatimuksia mobiilisovelluksille. Lääkinnällinen laite tai sovellus voidaan tuoda markkinoille Suomen alueella vain, jos siinä on CE-merkintä. Jotta CE-merkintä voidaan liittää sovellukseen, sovelluksen on täytettävä sille laeissa ja direktiiveissä asetetut vaatimukset, laitteelle tulee suorittaa kliininen arviointi, laite tulee testata, siitä tulee luoda tarvittavat asiakirjat ja ilmoitukset ja se tulee rekisteröidä Valviran ylläpitämään laiterekisteriin. Terveydenhuollon sovelluksissa tulee myös ertyisesti panostaa tietoturvaan. Terveysteknologia-alan peruslähtökohta on, että laitteen turvallisuudessa, suorituskyvyssä ja vaikuttavuudessa ei voida tehdä kompromisseja (4). Potilaan etu on ehdoton ja laitteen on sovelluttava käyttötarkoitukseensa (4). Huono tietoturva saattaa pahimmassa tapauksessa asettaa potilaan hengenvaaraan.

Mobiilisovellusten kehitys eroaa muiden ohjelmien kehityksestä monin tavoin. Mobiilisovellusten alustat, teknologiat ja jakelukanavat ovat omanlaisensa. Mobiililaitteet alustana mahdollistavat monenlaisten eri ominaisuuksien käyttämisen, joita muista laitteista ei välttämättä löydy, mutta rajoittavat myös sovelluksia pienen koon, kommunikaatioväylien ja laitteen tehojen takia. Kaksi suurinta mobiilikäyttöjärjestelmää ovat Applen iOS ja Googlen Android. Molemmat käyttöjärjestelmät tarjoavat kehittäjille kehitykseen työkalut ilmaiseksi, mutta vaativat maksua kehitystunnuksista. Kehitystunnuksilla kehittäjä saa käyttöönsä erilaisia teknologioita ja ominaisuuksia. Kehitystunnuksia tarvitaan, jos halutaan julkaista sovellus käyttöjärjestelmien virallisissa sovelluskaupoissa. Viralliset sovelluskaupat ovat App Store iOS käyttöjärjestelmälle ja Play Store Android käyttöjärjestelmälle. Molemmille käyttöjärjestelmille löytyy epävirallisia sovelluskauppoja ja sovelluksia voi myös julkaista itsenäisesti.

Mobiilisovelluksia voidaan kehittää usealla eri teknologialla. Sovelluskehittäjän on valittava teknologioista se, joka sopii sovelluksen ominaisuuksiin ja käyttökohteeseen parhaiten. Jokaisella teknologialla on omat vahvuutensa, heikkoutensa ja erityispiirteensä. Tek-

nologiat voidaan jakaa karkeasti kolmeen eri kategoriaan: natiivi, hybridi ja web. Natiivilla teknologialla tarkoitetaan alustan oman ohjelmointikielen käyttämistä sovelluksen kehittämiseen. Ne tarjoavat näistä kolmesta parhaiten pääsyn laitteen alustaan ja komponentteihin ja siksi mahdollistavat parhaan käytettävyyden, käyttökokemuksen ja järjestelmän omien ainutlaatuisten piirteiden mukaisen toteutuksen. Niiden heikkouksia hitaampi ja työläämpi kehitys. Natiivit sovellukset toimivat vain yhdellä käyttöjärjestelmällä, eli usealla käyttöjärjestelmälle kehittäessä tulee joka alustalle tehdä eri sovellukset eri ohjelmointikielellä. Tunnetuimpia natiiveja teknologioita ovat esimerkiksi ohjelmointikielet Swift ja Objective-C, joita käytetään sovellusten kehittämiseen Applen tuotteille ja ohjelmointikieli Java, jota käytetään Android-pohjaisille laitteille kehittämiseen. Webteknologiat käyttävät kehitykseen webohjelmointiin tarkoitettuja teknologioita, kuten HTML5, JavaScript ja CSS. Webteknologioiden vahvuus on koodin jakaminen alustojen välillä ja koodin toimiminen suurilta osin samalla lailla joka alustalla. Webteknologioiden heikkouksia on muun muassa vajaa pääsy laitteen komponentteihin, monikosketusominaisuuksien toteuttamisen vaikeus ja huonompi tehokkuus. Hybriditeknologioissa käytetään yhdessä natiiveja teknologioita ja webteknologioita. Ne koostuvat yleensä ohuesta natiiveilla teknologioilla luodusta pohjasta, jonka päällä ajetaan webteknologoilla tuotettuja ominaisuuksia. Hybridin suurin hyöty on siinä, että samaa koodia voidaan käyttää eri alustoilla ja päästään myös käsiksi laitteen sisäisiin komponentteihin. Hybriditeknologioiden huonoja puolia on yhdistelmä natiivien teknologioiden ja webteknologioiden huonoista puolista.

Mobiililaitteiden erityispiirteet luovat mobiilikehitykseen sille luonteenomaisia haasteita. Nämä haasteet on otettava huomioon jo suunnitteluvaiheessa. Mobiililaitteiden pieni koko asettaa rajoitteita niihin asennettavien komponenttien kanssa ja kaiken kaikkiaan niiden kapasiteetit ovat usein pienempiä kuin tietokoneilla. Hyödyntämällä ominaisuuksia kuten eleet, kosketus, sormenjäljen tunnistaminen, kamera, sijainnin seuraaminen, kiihtyvyyden ja liikkeen tunnistus, voidaan luoda hyviä käyttöliittymiä ja paikata osaa rajoitteista. Rajallisia resursseja voidaan paikata pilvipalvelujen avulla. Pilvipalvelut ovat Internet-yhteyden kautta aina tarpeen vaatiessa käytettäviä tietoteknisiä resursseja, kuten verkkoja, palvelimia, muistia, sovelluksia ja palveluita. Mobiililaitteiden langattomat siirtonopeudet vaihtelevat alustasta, liittymästä ja käyttäjän sijainnista riippuen. Huonoihin yhteyksiin voidaan varautua tallentamalla tarvittava data laitteeseen ja päivittämällä se yhteyden löytyessä. Mobiilisovelluksille on korkeat laatuvaatimukset ja niiden tulee usein toimia usealla eri alustalla. Alustasta riippumatta sovellukselle tulee luoda yhtenäinen käyttöliittymä, mutta samalla ottaa huomioon alustan ainutlaatuiset piirteet ja muotoilut.

Mobiililaitteiden tietoturvariskit ovat monin tavoin samanlaisia kuin muilla tietotekniikkaan liittyvillä osa-alueilla, mutta ainutlaatuisen luonteensa takia on olemassa joitakin mobiililaitteille ominaisia tietoturvaan liittyviä piirteitä. Uhkaa nostavia ominaisuuksia ovat esimerkiksi pieni koko, mahdollisuus liikkua käyttäjän mukana, Jailbreak- tai Root-

operaatio ja datan suuri määrä ja keskittyminen laitteessa. Tietoturva on otettava huomioon jo kehitysvaiheessa, jotta mahdolliset haavoittuvuudet voidaan estää. Kehitysvaiheessa voidaan käyttää sovelluksen skannausta tietoturvan parantamiseen. Sovelluksen skannaus koostuu yleensä staattisesta sisäistestauksesta ja dynaamisesta ulkoistestauksesta.

Mobiililaitteet omaavat usein monia eri keinoja olla vuorovaikutuksessa ympäröivän maailman kanssa. Erilaisten verkkoyhteyksien ja muistinkäsittelykeinojen, kuten Wi-Fin, Bluetoothin, puhelinverkon, muistikorttien ja pilvisäilöjen takia tarvitaan entistä enemmän suojautumiskeinoja luvattoman pääsyn ja datan menetyksen estämiseksi. Kolmannen osapuolen sovelluksia voidaan ladata mobiililaitteisiin sovelluskaupoista tai muista lähteistä. Vaikka sovellukset itsessään eivät olisi haittaohjelmia, ne saattavat sisältää tietoturva-aukkoja, joita haitalliset tahot voivat hyödyntää. Liian monimutkainen tai laitteen käyttöä estävä tietoturvapolitiikka haittaa käyttäjää ja pahimmassa tapauksessa ajaa käyttäjän etsimään mahdollisuuksia tietoturvan toteuttavien kokonaisuuksien kiertämiseen. Mobiiliuhkia ovat haitalliset ohjelmat ja hyökkäykset. Mobiilihaittaohjelma on ohjelma tai skripti, joka on suunniteltu häiritsemään mobiililaitteita, keräämään arkaluontoista informaatiota tai saamaan luvaton pääsy laitteelle. Hyökkäykset eroavat haitallisista ohjelmaista siten, että ne eivät välttämättä tarvitse erillistä ohjelmaa käyttäjän laitteelle aiheuttaakseen haittaa. Mobiililaitteita vastaan tehtyjä hyökkäyksiä ovat esimerkiksi sosiaalinen tiedustelu, SQL-injektio, istunnon kaappaus, palvelunesto hyökkäys ja QR-koodi huijaus.

Mobiililaitteiden ainutlaatuisten ominaisuuksien takia niissä ei välttämättä toimi kaikki vanhat tunnistusmetodit, mutta ne tuovat monta uutta vaihtoehtoa. Voidaan esimerkiksi tunnistaa kameralla silmän retina, 3-D kasvot, silmien räpäytyssarja, käden muoto ja sormenjälki. Kosketusnäyttöä hyödyntäen tunnistautuminen voi olla esimerkiksi näytöllä tietyn kuvion paineleminen, sormella kuvion piirtäminen, allekirjoituksen tekeminen, tietyn nopeuden ja voiman käyttö kuvion jäljentämisessä tai eleillä kuvion tekeminen. Mobiililaitteet ja niiden ympäristö sisältävät erityisiä ominaisuuksia, jotka voivat lisätä tietovuodon riskiä. Kaikki arkaluontoinen laitteeseen tallennettu data pitäisi olla mahdollista salata. Data voidaan suojata myös eristämällä, käärimällä tai virtualisoimalla. Tärkein mobiiliverkon suojausmekanismi on virtuaalinen mobiiliyksityisverkko. Mobiililaitteita ja niiden sovelluksia voidaan myös hallita mobiililaitteiden tai sovellusten keskitetyllä hallintaohjelmalla.

6. ARVIOINTI

Työ tehtiin todellisen tarpeen mukaan. Alkuperäinen aiheen rajaus oli mobiiliteknologiat, mutta sitä vaihdettiin myöhemmin käsittämään koko mobiilisovellusten kehitysprosessi. Ennen aiheen vaihtoa työ oli jo keretty aloittaa ja tekstiäkin oli tuotettu jo kohtalaisesti. Aiheen vaihto aiheutti ongelmia työn aikataulussa, sillä kaikkea aiemmin tutkittua ja kirjoitettua ei voitu käyttää. Muutamaa lukua lukuun ottamatta koko työ tuli aloittaa alusta. Aiheen vaihto antoi kuitenkin kirjoittajalle pienen näytteen siitä mitä kirjoittaminen tulisi olemaan ja kuinka teksti muodostuu työn edetessä. Tästä oli luultavasti apua uuden aiheen rakennetta luodessa. Esimerkkeinä työn mahdollisista käsittelyaiheista esitettiin terveydenhuollon vaatimukset, alustat ja laitteet, mobiililaitteiden verkot ja pilvipalvelut, sekä julkaisu. Erityiskohteena oli terveydenhuollon mobiilisovellukset. Tarkoituksena oli saada yleiskuva mitä mobiilisovellusten kehitykseen liittyy ja mitä tulee ottaa huomioon, kun mobiilisovelluksia tehdään terveydenhuollon tarpeisiin. Toimeksiantaja ei tarvinnut yksityiskohtaista selontekoa eri osioista. Kaiken kaikkiaan työn tavoitte saavutettiin.

Lähteitä oli aluksi vaikea löytää. Kun työn rakenne ja eri osiot alkoivat hahmottua, niin lähteitä löytyi hyvin, koska hauissa voitiin käyttää tarkempia hakutermejä. Työn edetessä lähteitä käytettiin laajasti. Lähteiden hakuun käytettiin useita eri kanavia, kuten Tampereen teknillisen yliopiston kirjaston haku (kirjat ja tieteelliset artikkelit), työn tarkastajan ja asiantuntujoiden suositukset, Internethaut ja suorat kyselyt, esimerkiksi Euroopan Unionilta. Usean eri kanavan käyttö vähentää riskiä, että asioita olisi tarkasteltu yksipuolisesti. Ennen työn tekemistä kirjoittajalla ei ollut suurempaa kokemusta mobiilisovellusten ohjelmoinnista. Jos kirjoittajalla olisi enemmän kokemusta aiheesta ennen työn kirjoittamista, niin työ olisi ollut helpompi suunnitella ja kirjoittaa. Kirjoittajalla oli kuitenkin hyvä mahdollisuus kirjoittaa työ suunnattuna samalla osaamistasolla olevalle lukijalle.

Aihe oli laaja, joten työstä tuli myös hieman hajanainen. Työn eri osiot eivät aina liity yhteen luonnollisesti ja osa asioista kuului monen eri luvun aihepiiriin. Esimerkiksi tietoturva on olennainen osa terveydenhuollon sovelluksia, mutta myös suuri osakohta mobiilisovellusten kehitystä yleisesti. Mobiililaitteilla sisäänkirjautuminen on toteutettava erilailla kuin pöytäkoneissa mobiilaitteiden pienen koon takia, joten sitä käsiteltiin ”Mobiililaitteiden pienet resurssit” luvussa. Se on kuitenkin myös tietoturvaan liittyvä tekijä. Jos sisäänkirjautumisesta tehdään liian haastava, niin käyttäjä saattaa kiertää sen ja siitä koituu tietoturvariski. Tämän takia samaa aihepiiriä on käsitelty ”Käyttäjän tunnistus ja pääsynhallinta” luvussa. Työn aiheessa ei määritetty keskitytäänkö kokonaan uusiin mobiilisovelluksiin vai vanhoja järjestelmiä käyttäviin mobiilisovelluksiin. Rajaamalla työ vain toiseen näistä olisi siitä saatu tiiviimpi. Työhön olisi voinut lisätä haastatteluja tai tosielämän esimerkkejä. Toisaalta ei ole tietoa olisiko näitä voitu jättää julkiseen versioon työstä. Olisi myös voitu toteuttaa oma mobiilisovelluksen kehitysprojekti kokeellisena

tutkimuksena, jonka kautta olisi voitu huomata mobiilisovellusten kehittämisen ominaisuuksia ja ongelmia, sekä etsiä niihin ratkaisuja. Työn kannalta hyöty tällaisesta projektista olisi saattanut kuitenkin olla kirjoittajan kokemustason takia vähäinen. Ongelmat, joita mahdollisesti olisi kohdattu, olisivat olleet hajanaisia ja niistä ei olisi välttämättä saatu koottua kokonaiskuvaa. Ongelmiin vastausten löytäminen projektin ja oman tekemisen kautta olisivat olleet kokemustason takia kyseenalaisia. Työssä on kokeellisen tutkimuksen sijaan kerätty tietoa muilta ammattilaisilta ja tieteellisistä julkaisuista. Tällä tavalla saatiin paremmin selville mobiilikehityksen ongelmat, niiden syyt ja ratkaisuvaihtoehdot. Nämä ratkaisut olisi kuitenkin voinut yhdistää, jotta teoriapainotteinen työ olisi saanut konkreettisia esimerkkejä.

LÄHTEET

1. Nicol. Mobile Strategy: How Your Company Can Win by Embracing Mobile. s.l. : IBM Press, 2013. 9780133094916.

2. Valcke. Best practices in mobile security. Biometric Technology Today. 2016, Osa/vuosik. 2016, 3.

3. Sydow. Record Levels of App Downloads & App Store Consumer Spend in Q4 2017. App Annie. [Online] 25. 1. 2018. [Viitattu: 22. 3. 2018.] https://www.appannie.com/en/insights/market-data/app-downloads-consumer-spend-q4-2017/.

4. Ståhlberg. Terveydenhuollon laitteiden lakisääteiset määräykset kansainvälisillä markkinoilla. Suomi ja EU fokuksessa. Business Finland. [Online] 14. 1. 2015. [Viitattu: 11. 1. 2018.] https://www.businessfinland.fi/globalassets/julkaisut/terveydenhuollon_laitteiden_lakisaateiset_maaraykset_opas.pdf. ISBN 978-952-457-587-4.

5. Grönlund, Raitoharju, Ranti, Seppälä, Ståhlberg. Suomen terveysteknologia-alan nykytila ja haasteet. Business Finland. [Online] 2017. [Viitattu: 1. 3. 2018.] https://www.businessfinland.fi/globalassets/julkaisut/suomen_terveysteknologia-alan_nykytila_ja_haasteet.pdf. 978-952-457-634-5.

6. Enersoft. Enersoft. [Online] Enersoft Oy. [Viitattu: 16. 3. 2017.] http://www.enersoft.fi.

7. Pujolle. Health care on mobile devices. Paris: Springer Paris, 2016. 1958-9395.

8. Google Fit - Fitness Tracking. Google Play. [Online] Google LLC. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.google.android.apps.fitness&hl=en.

9. Health. Apple Health. [Online] Apple Inc. [Viitattu: 27. 7. 2017.] https://www.apple.com/lae/ios/health/.

10. Samsung. Samsung Health. Samsung. [Online] Samsung. [Viitattu: 25. 7. 2018.] https://www.samsung.com/us/support/owners/app/samsung-health.

11. Wazid, Zeadally, Das, Odelu. Analysis of Security Protocols for Mobile Healthcare. s.l. : Journal of Medical Systems, 2016. 0148-5598.

12. Intille. A new research challenge: persuasive technology to motivate healthy aging. 3, Massachusetts : IEEE, 2004, Osa/vuosik. 8. 1089-7771.

13. Klasnja, Pratt. Healthcare in the pocket: Mapping the space of mobile-phone health interventions. 1, s.l. : Elsevier Inc., Helmikuu 2012, Journal of Biomedical Informatics, Osa/vuosik. 45, ss. 184-198. 1532-0464.

14. Kim, Beresford, Stajano. Towards a Security Policy for Ubiquitous Healthcare Systems (Position Paper). Berlin : Springer, Berlin, Heidelberg, 2007. 978-3-540-71788-1.

15. Morgan, Agee. Mobile Healthcare. 2, s.l. : Frontiers of Health Services Management, 2012, Osa/vuosik. 29. 0748-8157.

16. Wu, Wang, Lin. What Drives Mobile Health Care? An Empirical Evaluation of Technology Acceptance. Havaiji : IEEE, 2005. 0-7695-2268-8.

17. BinDhim, Trevena. There's an App for That: A Guide for Healthcare Practitioners and Researchers on Smartphone Technology. 2, s.l. : Online Journal of Public Health Informatics, 2015, Online Journal of Public Health Informatics, Osa/vuosik. 7. 1947-2579.

18. Boukerche, Ren. A secure mobile healthcare system using trust-based multicast scheme. 4, s.l. : IEEE, 2009, Osa/vuosik. 27. 0733-8716.

19. 2 Billion Consumers Worldwide to Get Smart(phones) by 2016. eMarketer. [Online] eMarketer, 11. 12. 2014. [Viitattu: 4. 7. 2017.] https://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694.

20. Ventä, Isomursu, Ahtinen. "My Phone is a Part of My Soul" – How People Bond with Their Mobile Phones. Valencia, Spain : IEEE, 2008. 978-0-7695-3367-4.

21. Glaros, Fotiadis. Wearable Devices in Healthcare. Jain, Ichalkaranje, Jain, Silverman. Intelligent Paradigms for Healthcare Enterprises. Berlin : Springer, Berlin, Heidelberg, 2005.

22. Bravo-Escobar, González-Represas, Gómez-González, Montiel-Trujillo, Aguilar-Jimenez, Carrasco-Ruíz, Salinas-Sánchez. Effectiveness and safety of a home-based cardiac rehabilitation programme of mixed surveillance in patients with ischemic heart disease at moderate cardiovascular risk: A randomised, controlled clinical trial. s.l. : BMC, 2017. 1471-2261.

23. Rubel, Fayn, Nollo, Assanelli, Li, Restier, Adami, Arod, Atoui, Ohlsson, Simon-Chautemps, Télisson, Malossi, Ziliani, Galassi, Edenbrandt, Chevalier. Toward personal

eHealth in cardiology. Results from the EPI-MEDICS telemedicine project. 4, s.l. : Journal of Electrocardiology, 2005, Osa/vuosik. 38.

24. Flowers or a robot army?: Encouraging awareness & activity with personal, mobile displays. Consolvo, Klasnja, McDonald, Avrahami, Froehlich, LeGrand, Libby, Mosher, Landay. Soul : ACM, 2008. 978-1-60558-136-1.

25. MediNet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony. Mohan, Marin, Sultan, Deen. Vancouver : Engineering in Medicine and Biology Society, 2008. 978-1-4244-1814-5.

26. Weight Watchers. App Store. [Online] Weight Watchers International Inc. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/us/app/weight-watchers/id331308914?mt=8.

27. Weight Watchers Mobile. Google Play. [Online] Weight Watchers International Inc. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.weightwatchers.mobile&hl=en.

28. Lose It! - Calorie Counter. Google Play. [Online] FitNow Inc. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.fitnow.loseit&hl=en.

29. Lose It! – Calorie Counter. App Store. [Online] FitNow. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/us/app/lose-it!-weight-loss-program/id297368629.

30. MyFitnessPal. App Store. [Online] MyFitnessPal.com. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/us/app/calorie-counter-diet-tracker/id341232718?mt=8&ign-mpt=uo%3D4.

31. Calorie Counter - MyFitnessPal. Google Play. [Online] MyFitnessPal, Inc. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.myfitnesspal.android&hl=en.

32. Pact: Earn Cash for Exercise and Healthy Living. App Store. [Online] GymPact. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/us/app/gympact-cash-reward-to-motivate/id456068701?mt=8.

33. Pact: Earn Cash for Exercising. Google Play. [Online] Pact Team. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.gympact.android.

34. Fooducate. App Store. [Online] Fooducate, Ltd. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/us/app/fooducate/id398436747?mt=8&ign-mpt=uo%3D4.

35. Fooducate. Google Play. [Online] Fooducate, Ltd. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.fooducate.nutritionapp.

36. Nike+ Training Club - Workouts & Fitness Plans. Google Play. [Online] Nike Inc. [Viitattu: 27. 7. 2017.] https://play.google.com/store/apps/details?id=com.nike.ntc.

37. Nike+ Training Club. App Store. [Online] Nike Inc. [Viitattu: 27. 7. 2017.] https://itunes.apple.com/app/nikewomen-training-club/id301521403.

38. Arkistolaki. Finlex. [Online] 23. 9. 1994. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/1994/19940831.

39. Henkilötietolaki. Finlex. [Online] 22. 4. 1999. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/1999/19990523.

40. Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista. Finlex. [Online] 22. 9. 2000. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/2000/20000812.

41. Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista. Finlex. [Online] 21. 8. 2009. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/2009/20090661.

42. Laki viranomaisten toiminnan julkisuudesta. Finlex. [Online] 21. 5. 1999. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

43. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Finlex. [Online] 9. 2. 2007. [Viitattu: 20. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/2007/20070159.

44. Valvira. Valvira. [Online] 19. 4. 2016. [Viitattu: 7. 2. 2017.] http://www.valvira.fi/valvira.

45. Laki Sosiaali- ja terveysalan lupa- ja valvontavirastosta. Finlex. [Online] 31. 10. 2008. [Viitattu: 7. 2. 2017.] http://www.finlex.fi/fi/laki/ajantasa/2008/20080669.

46. Valviralle tehtävät ilmoitukset. Valvira. [Online] 9. 6. 2015. [Viitattu: 5. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/valviralle-tehtavat-ilmoitukset.

47. Terveysteknologia. Valvira. [Online] 15. 9. 2009. [Viitattu: 5. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia.

48. Tuotteen markkinoille saattaminen. Valvira. [Online] 29. 9. 2009. [Viitattu: 7. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen.

49. CE-merkintä. Europa. [Online] 12. 6. 2017. [Viitattu: 18. 12. 2017.] https://europa.eu/youreurope/business/product/ce-mark/index_fi.htm.

50. Manufacturers. Europa. [Online] 19. 12. 2017. [Viitattu: 19. 12. 2017.] https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en.

51. Laki terveydenhuollon laitteista ja tarvikkeista. Finlex. [Online] 24. 6. 2010. [Viitattu: 13. 11. 2017.] http://www.finlex.fi/fi/laki/alkup/2010/20100629.

52. Salminen. EU ja CE-merkki. University of Eastern Finland. [Online] 19. 3. 2013. [Viitattu: 13. 11. 2017.] https://www2.uef.fi/documents/976466/1745345/06-19Salminen+EU+CE/945a3d50-9925-4aac-977a-8546cdb44450.

53. Neuvoston direktiivi 93/42/ETY. Europa. [Online] 14. 6. 1993. [Viitattu: 13. 11. 2017.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:fi:PDF.

54. Euroopan parlamentin ja neuvoston direktiivi 98/79/EY. Europa. [Online] 27. 10. 1998. [Viitattu: 23. 11. 2017.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:331:0001:0037:fi:PDF.

55. Neuvoston direktiivi 90/385/ETY. Europa. [Online] 20. 6. 1990. [Viitattu: 23. 11. 2017.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1990L0385:20071011:fi:PDF.

56. Terveydenhuollossa käytettävien itsenäisten ohjelmistojen määrittely- ja luokitteluohje lääkinnällisten laitteiden sääntelyn puistteissa. Valvira. [Online] 1. 2012. [Viitattu: 13. 11. 2017.] https://www.valvira.fi/documents/14444/37132/sw_luokitteluohje_2012-03-13.pdf.

57. Ohjelmistot ja tietojärjestelmät. Valvira. [Online] 10. 7. 2015. [Viitattu: 13. 9. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tietojarjestelmat.

58. Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. Europa. [Online] 15. 7. 2016. [Viitattu: 12. 2. 2018.] https://ec.europa.eu/docsroom/documents/17921.

59. Euroopan parlamentin ja neuvoston direktiivi 2007/47/EY. Europa. [Online] 5. 9. 2007. [Viitattu: 19. 4. 2018.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:fi:PDF.

60. Käyttötarkoituksen määrittely. Valvira. [Online] 29. 9 2009. [Viitattu: 7. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/kayttotarkoituksen_maarittely_ja_luokittelu.

61. Guidance document - Classification of Medical Devices - MEDDEV 2.4/1 rev.9. Europa. [Online] 18. 5. 2015. [Viitattu: 15. 11. 2017.] http://ec.europa.eu/DocsRoom/documents/10337/attachments/1/translations.

62. Partanen, Knuuttila. Terveydenhuollon laitteen ja tarvikkeen vaatimustenmukaisuuden arviointi. Valvira. [Online] 18. 3. 2011. [Viitattu: 24. 11. 2017.] http://www.valvira.fi/documents/14444/37132/Maarays_1_2011.pdf.

63. Terveydenhuollon laitteen ja tarvikkeen vaatimustenmukaisuuden arviointi. Valvira. [Online] 18. 3. 2011. [Viitattu: 18. 12. 2017.] http://www.valvira.fi/documents/14444/37132/Maarays_1_2011.pdf.

64. CE-merkintä. Valvira. [Online] 12. 10. 2009. [Viitattu: 13. 11. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/ivd_-laitteet/ce-merkinta.

65. Partanen, Aarnikka. CE-merkinnän käyttö terveydenhuollon laitteessa ja tarvikkeessa. Valvira. [Online] 18. 3. 2011. [Viitattu: 8. 3. 2018.] http://www.valvira.fi/documents/14444/37132/Maarays_2_2011.pdf.

66. Terveyspalvelujen ohjaus ja valvonta. Aluehallintovirasto. [Online] 4. 9. 2014. [Viitattu: 13. 9. 2017.] https://www.avi.fi/web/avi/terveyspalvelujen-ohjaus-ja-valvonta#.WbkMkMgjGUk.

67. Olennaiset vaatimukset. Valvira. [Online] 12. 10. 2009. [Viitattu: 7. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/olennaiset_vaatimukset.

68. Merkinnät ja käyttöohjeet. Valvira. [Online] 12. 10. 2009. [Viitattu: 7. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/merkinnat_ja_kayttoohjeet.

69. Kliininen arviointi. Valvira. [Online] 12. 10. 2009. [Viitattu: 7. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/kliiniset_laitetutkimukset.

70. Partanen, Linnavuori. Terveydenhuollon laitteilla ja tarvikkeilla tehtävät kliiniset tutkimukset. Valvira. [Online] 6. 9. 2010. [Viitattu: 2. 3. 2018.] https://www.finlex.fi/data/normit/39644/maarays_3_2010_kliininen_laitetutkimus.pdf.

71. Nando (New Approach Notified and Designated Organisations) Information System. Europa. [Online] Euroopan komissio, 18. 12. 2017. [Viitattu: 19. 12. 2017.] http://ec.europa.eu/growth/tools-databases/nando/.

72. Vaatimustenmukaisuuden arviointi. Valvira. [Online] 9. 10. 2009. [Viitattu: 19. 12. 2017.] http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/terveydenhuollon_laitteet_ja_tarvikkeet/vaatimustenmukaisuuden_arviointi.

73. Mobile Operating System Market Share Worldwide. Statcounter. [Online] 6. 2018. [Viitattu: 26. 7. 2018.] http://gs.statcounter.com/os-market-share/mobile/worldwide.

74. Program Membership Details. Apple Developer. [Online] Apple Inc. [Viitattu: 24. 8. 2017.] https://developer.apple.com/programs/whats-included/.

75. How the Program Works. Apple Developer. [Online] Apple Inc. [Viitattu: 23. 8. 2017.] https://developer.apple.com/programs/how-it-works/.

76. App Analytics. Apple Developer. [Online] Apple Inc. [Viitattu: 24. 8. 2017.] https://developer.apple.com/app-store/app-analytics/.

77. Launching Your App on Devices. Apple Developer. [Online] Apple Inc. [Viitattu: 28. 9. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/LaunchingYourApponDevices/LaunchingYourApponDevices.html.

78. How to use the Play Console. Play Console Help. [Online] Google LLC. [Viitattu: 23. 8. 2017.] https://support.google.com/googleplay/android-developer/answer/6112435?hl=en.

79. Set up alpha/beta tests. Play Console Help. [Online] [Viitattu: 12. 9. 2017.] https://support.google.com/googleplay/android-developer/answer/3131213.

80. Sinicki. Developing for Android vs developing for iOS – in 5 rounds. Android Authority. [Online] Android Authority, 9. 6. 2016. [Viitattu: 21. 3. 2018.] https://www.androidauthority.com/developing-for-android-vs-ios-697304/.

81. My Android. Anroid. [Online] Google LLC. [Viitattu: 22. 3. 2018.] https://www.android.com/myandroid/.

82. Beal. Android launcher. Webopedia. [Online] QuinStreet Inc. [Viitattu: 22. 3. 2018.] https://www.webopedia.com/TERM/A/android_launcher.html.

83. What's New in Notifications. Apple Developer. [Online] Apple Inc., 2015. [Viitattu: 28. 9. 2017.] https://developer.apple.com/videos/play/wwdc2015/720/.

84. Notifications. Android Developer. [Online] Google LLC. [Viitattu: 28. 9. 2017.] https://developer.android.com/guide/topics/ui/notifiers/notifications.html.

85. Korf, Oksman. "Native, HTML5, or Hybrid: Understanding Your Mobile Application Development Options". Salesforce sevelopers. [Online] 6. 2016. [Viitattu: 10. 10. 2017.] https://developer.salesforce.com/page/Native,_HTML5,_or_Hybrid:_Understanding_Your_Mobile_Application_Development_Options.

86. Charkaoui, Lahmar, Marzak, Abdelbaki. Cross-platform Mobile Development based on MDA Approach. International Journal of Interactive Mobile Technologies. 2016, Osa/vuosik. 10, 4.

87. Native, Web or Hybrid Apps? What's The Difference. MobiLoud. [Online] [Viitattu: 23. 3. 2018.] https://www.mobiloud.com/blog/native-web-or-hybrid-apps/.

88. Colao. Facebook's HTML5 Dilemma, Explained. Forbes. [Online] Forbes Media LLC, 19. 9. 2012. [Viitattu: 10. 4. 2018.] https://www.forbes.com/sites/jjcolao/2012/09/19/facebooks-html5-dilemma-explained/#22c611c4170a.

89. Occhino. React Native: Bringing modern web techniques to mobile. Facebook code. [Online] 26. 3. 2015. [Viitattu: 10. 10. 2017.] https://code.facebook.com/posts/1014532261909640/react-native-bringing-modern-web-techniques-to-mobile/.

90. Swift. Apple Developer. [Online] Apple Inc. [Viitattu: 21. 3. 2018.] https://developer.apple.com/swift/.

91. Thornsby. Working with WebView: displaying web content inside your Android app. Android Authority. [Online] 19. 12. 2016. [Viitattu: 28. 3. 2018.] https://www.androidauthority.com/working-with-webview-736873/.

92. WebView. Android Developer. [Online] Google LLC. [Viitattu: 2. 4. 2018.] https://developer.android.com/reference/android/webkit/WebView.html.

93. UIWebView. Apple Developer. [Online] Apple Inc. [Viitattu: 2. 4. 2018.] https://developer.apple.com/documentation/uikit/uiwebview.

94. Dann. Under the hood: Rebuilding Facebook for iOS. Facebook. [Online] 23. 8. 2012. [Viitattu: 14. 8. 2018.] https://www.facebook.com/notes/facebook-engineering/under-the-hood-rebuilding-facebook-for-ios/10151036091753920.

95. Angulo, Alonso, Ferre. UX & Cross-Platform Mobile Application Development Frameworks. Madrid : Madridin teknillinen yliopisto, 2014.

96. Eisenman. Learning React Native: Building Native Mobile Apps with JavaScript. s.l. : O'Reilly Media, 2016. 1491929006.

97. Android Market: Now available for users. Android Developers Blog. [Online] 22. 10. 2008. [Viitattu: 23. 8. 2017.] https://android-developers.googleblog.com/2008/10/android-market-now-available-for-users.html.

98. Apple Developer Program. Apple Developer. [Online] Apple Inc. [Viitattu: 23. 8. 2017.] https://developer.apple.com/programs/.

99. Burton. Android App Development for Dummies, 3rd Edition. s.l. : John Wiley & Sons, 2015. 9781119017929.

100. About App Distribution Workflows. Apple Developer. [Online] Apple inc. [Viitattu: 25. 8. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/Introduction/Introduction.html.

101. Configuring Your Xcode Project for Distribution. Apple Developer. [Online] Apple Inc. [Viitattu: 25. 8. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/ConfiguringYourApp/ConfiguringYourApp.html#//apple_ref/doc/uid/TP40012582-CH28-SW1.

102. Exporting Your App for Testing (iOS, tvOS, watchOS). Apple Developer. [Online] [Viitattu: 5. 9. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/TestingYouriOSApp/TestingYouriOSApp.html#//apple_ref/doc/uid/TP40012582-CH8-SW1.

103. iTunes Connect. Apple. [Online] [Viitattu: 5. 9. 2017.] https://www.apple.com/itunes/working-itunes/sell-content/connect/.

104. Submitting Your App to the Store. Apple Developer. [Online] [Viitattu: 5. 9. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/SubmittingYourApp/SubmittingYourApp.html#//apple_ref/doc/uid/TP40012582-CH9-SW1.

105. Submitting the App to App Review. Apple Developer. [Online] [Viitattu: 5. 9. 2017.] https://developer.apple.com/library/content/documentation/LanguagesUtilities/Conceptual/iTunesConnect_Guide/Chapters/SubmittingTheApp.html#//apple_ref/doc/uid/TP40011225-CH33.

106. App Review. Apple Developer. [Online] [Viitattu: 12. 9. 2017.] https://developer.apple.com/support/app-review/.

107. Transaction fees. Play Console Help. [Online] [Viitattu: 6. 9. 2017.] https://support.google.com/googleplay/android-developer/answer/112622?hl=en.

108. Kim. Creating Better User Experiences on Google Play. Android Developers Blog. [Online] [Viitattu: 12. 9. 2017.] https://android-developers.googleblog.com/2015/03/creating-better-user-experiences-on.html.

109. Upload an app. Play Console Help. [Online] [Viitattu: 7. 9. 2017.] https://support.google.com/googleplay/android-developer/answer/113469#store_listing.

110. Prepare & rollout releases. Play Console Help. [Online] [Viitattu: 8. 9. 2017.] https://support.google.com/googleplay/android-developer/answer/7159011.

111. Graphic assets, screenshots, & video. Play Console Help. [Online] [Viitattu: 7. 9. 2017.] https://support.google.com/googleplay/android-developer/answer/1078870.

112. Amazon. Amazon. [Online] Amazon.com Inc. [Viitattu: 27. 9. 2017.] https://www.amazon.com/.

113. Slide Me. Slide Me. [Online] Slide Me LLC. [Viitattu: 27. 9. 2017.] http://slideme.org/.

114. Freeman. Cydia. Cydia. [Online] [Viitattu: 3. 4. 2018.] http://cydia.saurik.com/.

115. AppCake. AppCake. [Online] AppCake. [Viitattu: 3. 4. 2018.] https://www.iphonecake.com/.

116. Publish Your App. Android Developer. [Online] Google LLC. [Viitattu: 27. 9. 2017.] https://developer.android.com/studio/publish/index.html.

117. Choosing a Membership. Apple Developer. [Online] [Viitattu: 6. 9. 2017.] https://developer.apple.com/support/compare-memberships/.

118. Distributing Apple Developer Enterprise Program Apps. Apple Developer. [Online] [Viitattu: 5. 9. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/DistributingEnterpriseProgramApps/DistributingEnterpriseProgramApps.html#//apple_ref/doc/uid/TP40012582-CH33-SW1.

119. Distributing Apps Outside the Mac App Store. Apple Developer. [Online] [Viitattu: 5. 9. 2017.] https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/DistributingApplicationsOutside/DistributingApplicationsOutside.html#//apple_ref/doc/uid/TP40012582-CH12-SW2.

120. Veikkaus Sovellukset. Veikkaus. [Online] Veikkaus Oy. [Viitattu: 11. 15. 2017.] https://www.veikkaus.fi/fi/sovellukset.

121. Müller. Designing native apps for Android and iOS: key differences and similarities. Cheesecakelabs. [Online] 20. 9. 2016. [Viitattu: 26. 3. 2018.] https://cheesecakelabs.com/blog/designing-native-apps-for-android-and-ios-key-differences-and-similarities/.

122. Perez. Niantic postpones its Pokémon GO events in Europe after its Chicago festival ended in disaster. TechCrunch. [Online] 31. 7. 2017. [Viitattu: 3. 10. 2017.] https://techcrunch.com/2017/07/31/niantic-postpones-its-pokemon-go-events-in-europe-after-its-chicago-festival-ended-in-disaster/.

123. Lehtiniitty. Pokémon GOn ensimmäisestä jättitapahtumasta tuli katastrofi – verkko- ja palvelinongelmat kaatoivat pelin. Mobiili.fi. [Online] 23. 7. 2017. [Viitattu: 3. 10. 2017.] http://mobiili.fi/2017/07/23/pokemon-gon-ensimmaisesta-jattitapahtumasta-tuli-katastrofi-verkko-ja-palvelinongelmat-kaatoivat-pelin/.

124. Heath. Pokémon Go's first real-world event was a disaster, and everyone was refunded. Business Insider. [Online] 22. 7. 2017. [Viitattu: 3. 10. 2017.] http://nordic.businessinsider.com/pokmon-go-chicago-event-issues-ticket-refunds-after-widespread-outage-2017-7.

125. Heath. What it was like to attend Pokémon Go's first real-world event that turned out to be a disaster. Business Insider. [Online] 25. 7. 2017. [Viitattu: 3. 10. 2017.] http://nordic.businessinsider.com/what-it-was-like-to-attend-pokmon-go-fest-event-in-chicago-2017-7.

126. Farokhmanesh. I went to pokémon go fest, and it was a disaster. The Verge. [Online] 25. 7. 2017. [Viitattu: 3. 10. 2017.] https://www.theverge.com/2017/7/25/16019404/pokemon-go-fest-refunds-disaster-review.

127. Flexispy. Flexispy. [Online] Flexispy, Ltd. [Viitattu: 29. 3. 2017.] https://www.flexispy.com/.

128. Viruses, Worms, and Trojans. Kabachinski. 1, Philadelphia : Biomedical Instrumentation & Technology, Tammikuu/Helmikuu 2005, Osa/vuosik. 39, ss. 46-48. Access number: 15742846. 08998205.

129. Grenoble. This Single Text Message Can Crash Your iPhone. Huffingtonpost. [Online] 27. 5. 2015. [Viitattu: 31. 3. 2017.] http://www.huffingtonpost.com/2015/05/27/text-message-crash-iphone-_n_7452324.html.

130. Eadicicco. Watch Out For This iPhone-Crashing Text Message. Time. [Online] 18. 1. 2017. [Viitattu: 18. 1. 2017.] http://time.com/4637574/iphone-crash-text-2017/.

131. Laki potilaan asemasta ja oikeuksista. Finlex. [Online] 17. 8. 1992. [Viitattu: 23. 11. 2017.] http://www.finlex.fi/fi/laki/ajantasa/1992/19920785#L4P13.

132. Ponemon. 2016 Ponemon Institute Cost of a Data Breach Study. SecurityIntelligence. [Online] 15. 6. 2016. [Viitattu: 23. 5. 2017.] https://securityintelligence.com/media/2016-cost-data-breach-study/.

133. Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices. s.l. : United States Department of Homeland Security, 2010.

134. Shaulov. Bridging mobile security gaps. Network Security. 2016, Osa/vuosik. 2016, 1.

135. Butterfield, Ngondi. A Dictionary of Computer Science. s.l. : Oxford University Press, 2016. 9780191768125.

136. Robust Defenses for Cross-Site Request Forgery. Barth, Jackson, Mitchell. Alexandria, Virginia : ACM New York, 2008. 978-1-59593-810-7.

137. Williams. Best antivirus for iPhone in 2018. Techradar. [Online] 30. 6. 2018. [Viitattu: 4. 7. 2018.] https://www.techradar.com/news/best-antivirus-for-iphone-in-2018.

138. Casey. Why Apple iPhones Don't Need Antivirus Software. Tom's guide. [Online] 14. 12. 2017. [Viitattu: 4. 7. 2018.] https://www.tomsguide.com/us/iphones-dont-need-antivirus-software,news-23111.html.

139. Song, Kim, Lee. The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. Mobile Information Systems. 2016, Osa/vuosik. 2016.

140. Jaakohuhta. MOT IT-Ensyklopedia. MOT IT-Ensyklopedia. [Online] [Viitattu: 9. 10 2017.]